



RIVISTA ITALIANA DI GEOPOLITICA

L'impero americano letto attraverso Internet
La sfida cinese e la guerriglia russa
Cyberwarfare, dove nessuno domina

LA RETE A STELLE E STRISCE

LIMES È IN EBOOK E IN PDF • WWW.LIMESONLINE.COM



€ 15,00



10/2018 • MENSILE



Guardare al futuro con la forza del passato

La nostra è una storia senza tempo che dura da 70 anni.
È il racconto di uomini e donne che hanno creduto nei propri sogni
e che hanno fatto vibrare il mondo con il coraggio e la curiosità.
Le loro idee sono diventate storia e oggi, forti della nostra preziosa
eredità, ci proiettiamo nel futuro con l'energia di chi è consapevole
di poter costruire nuove strade e raggiungere nuovi traguardi.

CONSIGLIO SCIENTIFICO

Rosario AITALA - Geminello ALVI - Marco ANSALDO - Alessandro ARESU - Giorgio ARFARAS - Angelo BOLAFFI
Aldo BONOMI - Edoardo BORJA - Mauro BUSSANI - Vincenzo CAMPORINI - Luciano CANFORA - Antonella
CARUSO - Claudio CERRETI - Gabriele CIAMPI - Furio COLOMBO - Giuseppe CUCCHI - Marta DASSÙ - Ilvo
DIAMANTI - Germano DOTTORI - Dario FABBRI - Augusto FANTOZZI - Tito FAVARETTO - Luigi Vittorio
FERRARIS - Federico FUBINI - Ernesto GALLI della LOGGIA - Carlo JEAN - Enrico LETTA - Ricardo Franco LEVI
Mario G. LOSANO - Didier LUCAS - Francesco MARGIOTTA BROGLIO - Fabrizio MARONTA - Maurizio
MARTELLINI - Fabio MINI - Luca MUSCARÀ - Massimo NICOLAZZI - Vincenzo PAGLIA - Maria Paola PAGNINI
Angelo PANEBIANCO - Margherita PAOLINI - Giandomenico PICCO - Romano PRODI - Federico RAMPINI
Andrea RICCARDI - Adriano ROCCUCCI - Sergio ROMANO - Gian Enrico RUSCONI - Giuseppe
SACCO - Franco SALVATORI - Stefano SILVESTRI - Francesco SISI - Mattia TOALDO - Roberto TOSCANO
Giulio TREMONTI - Marco VIGEVANI - Maurizio VIROLI - Antonio ZANARDI LANDI - Luigi ZANDA

CONSIGLIO REDAZIONALE

Flavio ALIVERNINI - Luciano ANTONETTI - Marco ANTONSICH - Federico ARGENTIERI - Andrée BACHOUD
Guido BARENDSON - Pierluigi BATTISTA - Andrea BIANCHI - Stefano BIANCHINI - Nicolò CARNIMEO
Roberto CARPANO - Giorgio CUSCITO - Andrea DAMASCELLI - Federico D'AGOSTINO - Emanuela C. DEL RE
Alberto DE SANCTIS - Alfonso DESIDERIO - Federico EICHBERG - Ezio FERRANTE - Wlodek GOLDKORN
Franz GUSTINCICH - Virgilio ILARI - Arjan KONOMI - Niccolò LOCATELLI - Marco MAGNANI - Francesco
MAIELLO - Luca MAINOLDI - Roberto MENOTTI - Paolo MORAWSKI - Roberto NOCELLA - Giovanni ORFEI
Federico PETRONI - David POLANSKY - Alessandro POLITI - Sandra PUCCINI - Benedetta RIZZO
Angelantonio ROSATO - Enzo TRAVERSO - Charles URJEWICZ - Pietro VERONESE - Livio ZACCAGNINI

REDAZIONE, CLUB, COORDINATORE RUSSIE

Mauro DE BONIS

DIRETTORE RESPONSABILE

Lucio CARACCIOLIO

HEARTLAND, RESPONSABILE RELAZIONI INTERNAZIONALI

Fabrizio MARONTA

COORDINATORE AMERICA

Dario FABBRI

COORDINATORE LIMESONLINE

Niccolò LOCATELLI

COORDINATRICE SCIENTIFICA

Margherita PAOLINI

CARTOGRAFIA E COPERTINA

Laura CANALI

COORDINATORE TURCHIA E MONDO TURCO

Daniele SANTORO

CORRISPONDENTI

Keith BOTSFORD (corrispondente speciale)

Afghanistan: Henri STERN - Albania: Ilir KULLA - Algeria: Abdennour BENANTAR - Argentina: Fernando
DEVOTO - Australia e Pacifico: David CAMROUX - Austria: Alfred MISSONG, Anton PELINKA, Anton
STAUDINGER - Belgio: Olivier ALSTEESEN, Jan de VOLDER - Brasile: Giancarlo SUMMA - Bulgaria: Antony
TODOROV - Camerun: Georges R. TADONKI - Canada: Rodolphe de KONINCK - Cechia: Jan KŘEN - Cina:
Francesco SISI - Congo-Brazzaville: Martine Renée GALLOY - Corea: CHOI YEON-GOO - Estonia: Jan
KAPLINSKIJ - Francia: Maurice AYMARD, Michel CULLIN, Bernard FALGA, Thierry GARCIN - Guy HERMET,
Marc LAZAR, Philippe LEVILLAIN, Denis MARAVAL, Edgar MORIN, Yves MÉNY, Pierre MILZA - Gabon: Guy
ROSSATANGA-RIGNAULT - Georgia: Gbia ZHORZHOLIANI - Germania: Detlef BRANDES, Iring FETSCHER,
Rudolf HILF, Josef JOFFE, Claus LEGGEWIE, Ludwig WATZAL, Johannes WILMS - Giappone: Kuzubiro JATABE
Gran Bretagna: Keith BOTSFORD - Grecia: Françoise ARVANITIS - Iran: Bijan ZARMANDILI - Israele: Arnold
PLANSKI - Lituania: Alfredas BLUMBLAUSKAS - Panamá: José ARDILA - Polonia: Wójciech GIEŁŻYŃSKI
Portogallo: José FREIRE NOGUEIRA - Romania: Emilia COSMA, Cristian IVANES - Ruanda: José KAGABO
Russia: Igor PELLICCIARI, Aleksej SALMIN, Andrej ZUBOV - Senegal: Momar COUMBA DIOP - Serbia e
Montenegro: Tijana M. DJERKOVIĆ, Miodrag LEKIĆ - Siria e Libano: Lorenzo TROMBETTA - Slovacchia:
Lubomir LIPTAK - Spagna: Manuel ESPADAS BURGOS, Victor MORALES LECANO - Stati Uniti: Joseph
FITCHETT, Igor LUKES, Gianni RIOTTA, Eva THOMPSON - Svizzera: Fausto CASTIGLIONE - Togo: Comi M.
TOULABOR - Turchia: Yasemin TAŞKIN - Città del Vaticano: Piero SCHIAVAZZI - Venezuela: Edgardo RICCIUTI
Ucraina: Leonid FINBERG, Miroslav POPOVIĆ - Ungheria: Gyula L. ORTUTAY

Rivista mensile n. 10/2018 (ottobre)
ISSN 2465-1494

Direttore responsabile

© Copyright

Lucio Caracciolo

GEDI Gruppo Editoriale SpA

via Cristoforo Colombo 90, 00147 Roma

GEDI Gruppo Editoriale SpA

Presidente onorario

Carlo De Benedetti

Consiglio di amministrazione

Presidente

Marco De Benedetti

Vicepresidenti

John Elkann, Monica Mondardini

Amministratore delegato

Laura Cioli

Consiglieri

Agar Brugiavini, Giacaranda Maria Caracciolo di Melito

Falck, Elena Ciallie, Alberto Clò, Rodolfo De Benedetti

Francesco Dini, Silvia Merlo, Elisabetta Oliveri

Luca Paravicini Crespi, Carlo Perrone, Michael Zaoui

Direttori centrali

Produzione e sistemi informativi *Pierangelo Calegari*

Relazioni esterne

Stefano Mignanego

Risorse umane

Roberto Moro

Divisione Stampa nazionale

Direttore generale

Corrado Corradi

Vicedirettore

Giorgio Martelli

Prezzo

15,00

Distribuzione nelle librerie: *Messaggerie Libri SpA, via Giuseppe Verdi 8, Assago (MI), tel. 02 45774.1 r.a. fax 02 45701032*

Responsabile del trattamento dati (dlgs 30 giugno 2003 n. 196) *Lucio Caracciolo*

Pubblicità *Ludovica Carrara, lcarrara@manzoni.it*

Informazione sugli abbonamenti: *GEDI Distribuzione SpA, Divisione abbonamenti Limes, casella postale 10642, 20110 Milano, tel. 199.78.72.78 (0864.256266 per chi chiama da telefoni cellulari il costo massimo della telefonata da rete fissa è di 14,26 cent di euro al minuto più 6,19 cent di euro alla risposta iva inclusa), fax 02.26681986, e-mail: abbonamenti@somedia.it*

Abbonamenti esteri: *tel. 0864.256266; arretrati: 199.78.72.78 (0864.256266 per chi chiama da telefoni cellulari; il costo massimo della telefonata da rete fissa è di 14,26 cent di euro al minuto più 6,19 cent di euro alla risposta iva inclusa). Non si effettuano spedizioni in contrassegno.*

La corrispondenza va indirizzata a *Limes - Rivista Italiana di Geopolitica, via Cristoforo Colombo 90, 00147 Roma, tel. 06 49827110; fax 06 49827125*

www.limesonline.com - limes@limesonline.com

GEDI Gruppo Editoriale SpA, Divisione Stampa nazionale, Banche dati di uso redazionale. In conformità alle disposizioni contenute nell'articolo 2 comma 2 del Codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica ai sensi dell'Allegato A del Codice in materia di protezione dei dati personali ex d.lgs. 30 giugno 2003 n. 196, GEDI Gruppo Editoriale SpA. rende noto che presso la sede di via Cristoforo Colombo 90, 00147 Roma esistono banche dati di uso redazionale. Per completezza, si precisa che l'interessato, ai fini dell'esercizio dei diritti riconosciuti dall'articolo 7 e seguenti del d.lgs. 196/03 - tra cui, a mero titolo esemplificativo, il diritto di ottenere la conferma dell'esistenza di dati, l'indicazione delle modalità di trattamento, la rettifica o l'integrazione dei dati, la cancellazione e il diritto di opporsi in tutto o in parte al relativo uso - potrà accedere alle suddette banche dati rivolgendosi al responsabile del trattamento dei dati contenuti nell'archivio sopraindicato presso la redazione di Limes, via Cristoforo Colombo 90, 00147 Roma.

I manoscritti inviati non saranno resi e la redazione non assume responsabilità per la loro perdita. *Limes* rimane a disposizione dei titolari dei copyright che non fosse riuscito a raggiungere

Registrazione al Tribunale di Roma n. 178 del 27/4/1993

Stampa e legatura Puntoweb s.r.l., stabilimento di Ariccia (Roma), novembre 2018

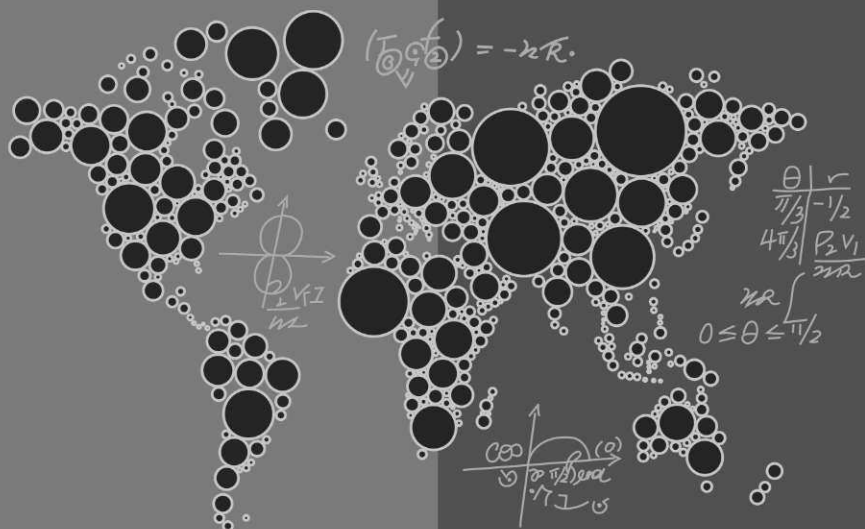
limes

RIVISTA ITALIANA DI GEOPOLITICA

L'impero americano letto attraverso Internet
La sfida cinese e la guerriglia russa
Cyberwarfare, dove nessuno domina

LA RETE A STELLE E STRISCE

LIMES È IN EBOOK E IN PDF • WWW.LIMESONLINE.COM



PARTE I

DOVE E COME GLI AMERICANI COMANDANO

- 9 DARIO FABBRI - L'impero informatico americano alla prova cinese
- 19 Frank PASQUALE - Se vincono gli algoritmi perde l'umanità
- 27 Dario FABBRI - Per una geopolitica umana applicata ai dati
- 35 Niccolò LOCATELLI - *Le fake news*, specchio dell'anima della Silicon Valley
- 45 Francesco VITALI GENTILINI - La strategia del cuculo, i giganti digitali vogliono prendersi tutto
- 53 Luca MAINOLDI - Washington e Silicon Valley non si amano ma spiano il mondo insieme
- 63 George FRIEDMAN - Il dilemma dell'Nsa

PARTE II

DOVE E COME SI DIFENDONO GLI ALTRI

- 71 Alessandro ARESU - Geopolitica della protezione
- 85 Giovanni COLLOT - Il Mercato unico serve, ma non basta
- 93 James LEWIS - Russia e Cina ci hanno scippato Internet
- 103 Simon TEMPLAR - Le conseguenze inintenzionali delle *fake news*
- 109 Alessandro ARESU - Per una biografia geopolitica di Telecom
- 123 Francesco MASELLI - La via francese alla sovranità digitale
- 131 Prabhu GUPTARA - In India Internet e modernità non sono sinonimi

PARTE III

CIBERGUERRA, TERRA DI NESSUNO?

- 139 Federico PETRONI - L'America all'offensiva cibernetica
- 149 Matthew CROSTON - Bot russi o americani pecoroni?
- 155 Giorgio CUSCITO - Il piano di Xi Jinping per superare gli Usa nell'intelligenza artificiale
(in appendice: Andrea GHIZZONI - 'In Cina, WeChat è Internet')
- 165 John BAMBENEK - Come la Russia proietta la sua potenza cibernetica
- 173 Matthew CROSTON - Per una gerarchia delle ciberpotenze
- 179 Luca MAINOLDI - La ciberfionda di David

LIMES IN PIÙ

- 189 **Pietro TINO - Se si ammala la pelle del pianeta**
197 **Sebastiano CONTRARI - AAA supereroi italici cercansi**

AUTORI

213

LA STORIA IN CARTE

a cura di Edoardo BORIA

215



LA RETE A STELLE E STRISCE


Parte I

DOVE e COME
gli **AMERICANI**
COMANDANO

L'IMPERO INFORMATICO AMERICANO ALLA PROVA CINESE

di Dario FABBRI

Internet è il versante virtuale del primato statunitense nel mondo. La Silicon Valley, malgrado l'afflato universalista, è intrinseca allo Stato federale e fornisce all'intelligence a stelle e strisce una quantità formidabile di dati. Chi si azzarda ad aprire a Pechino è perduto.

1.  NTERNET È UN FENOMENO PROFONDAMENTE americano, sottoposto all'interesse geopolitico della superpotenza, coincidente con il suo dominio planetario. Nella versione attuale è stato sviluppato da privati, ma è nato nel ventre militare degli Stati Uniti ed è tuttora funzionale alle esigenze strategiche del paese. La Silicon Valley fornisce all'Nsa e alla Cia innumerevoli dati per spiare alleati e antagonisti, ma non ha creato la tecnologia di cui dispone, non può esistere senza gli investimenti di Washington, non può sottrarsi alle imposizioni dell'amministrazione federale. Soprattutto, Internet è intrinseco alla globalizzazione, ovvero all'impero statunitense, ne è il versante virtuale, la dimensione parallela. Come il suo doppio strategico, la Rete globale è conseguenza diretta del crollo sovietico; dispone di matrice talassocratica attraverso i cavi posti sui fondali degli oceani; consente all'America di appropriarsi dell'intimità di miliardi di persone; impedisce alle altre nazioni d'essere realmente sovrane – comprese Russia e (parzialmente) Cina. Il suo futuro sarà inesorabilmente segnato dalla tenuta della supremazia statunitense, destini impossibili da sciogliere.

Come capita con le rotte marittime, il Web resterà universale fin quando Washington avrà la forza di imporsi sui suoi antagonisti. Soprattutto sulla Repubblica Popolare, impegnata a balcanizzarne l'estensione, attraverso l'esclusiva gestione dei server collocati in patria e la limitazione d'accesso per le società straniere. Attraverso il tentativo, tanto materiale quanto cibernetico, di usare l'intelligenza artificiale per legare a sé i potenziali satelliti, sviluppo altro delle nuove vie della seta. Offensiva cui l'America risponde con l'aggressione commerciale, raccontata come protezionismo, come (improbabile) tentativo di porre fine alla propria *pax*, in realtà centrata sulle capacità tecnologiche del rivale. Mentre i suoi apparati sono

impegnati a evitare che, in possesso di straordinaria liquidità e animati dalla brama di (ri)entrare nel mercato cinese, i giganti della Silicon Valley si pensino oltre le impellenze geopolitiche della nazione, finendo involontariamente per contribuire alla frantumazione di Internet. Con Trump quale insospettabile alfiere della società globale, determinato a puntellarne l'esistenza. Con il fine ultimo di mantenere intonsa la profondità informatica della propria grandezza.

2. Internet costituisce l'estensione artificiale del primato americano. Attraverso il virtuale la superpotenza gestisce l'unico mercato mondiale, mantiene connesse a sé le altre nazioni, controlla umori e intenzioni dell'ecumene. In sua assenza, conservare tanto sistema diventerebbe impervio, certamente più dispendioso. Il Web è universale dalla fine della guerra fredda, da quando l'amministrazione federale decise di diffondere all'estero un'invenzione già consumata nel 1969 in seno al Pentagono. Conferendole dimensione marittima.

Come il controllo delle rotte oceaniche è sostrato della globalizzazione¹ – su di esse viaggia oltre il 90% delle merci mondiali – un enorme reticolo di cavi sottomarini costituisce l'indispensabile ossatura dell'Internet globale. Oltre un milione di chilometri di condotte in fibra ottica, su cui corre il 99% dei dati scambiati in Rete, depositate sui fondali nel corso dei decenni. Con gli Stati Uniti quale centro geografico e strategico del sistema. Accezione fisica di una realtà che si vorrebbe inspiegabilmente immateriale – addirittura ribattezzata *cloud* (nuvola) in caso di deposito di memoria – perché irradiata attraverso microprocessori.

Come avviene con il mantenimento del libero passaggio negli istmi e negli stretti del pianeta, benché centinaia di tubi non le appartengano la superpotenza si sente depositaria della loro sicurezza, nonché del diritto di spiare il contenuto. Al punto da perlustrarli ciclicamente con la propria Marina e dichiararsi più volte preoccupata della (remota) possibilità che Russia, Cina e altri suoi sfidanti possano materialmente tagliarli, precipitando il mondo nel buio virtuale. Specie ora che le multinazionali americane impiantano cavi al ritmo di 100 mila chilometri l'anno – entro il 2019 soltanto Google costruirà tre fondamentali linee che collegheranno Los Angeles con il Cile (diretrice Curie), la Danimarca con l'Irlanda (Havfrue) e Guam con Hong Kong (Hkg).

Da molto prima di Internet Washington utilizza il mare per origliare le comunicazioni dei nemici. Negli anni Settanta i marines realizzarono l'operazione Ivy Bells per spiare i fili che dalle isole Curili conducevano in Unione Sovietica, prima che l'analista dell'Nsa Ronald Pelton raccontasse tutto al nemico per 35 mila dollari. Ancora nel 2005, in piena era digitale, fu varato il sottomarino *Jimmy Carter* in grado di rubare informazioni dai fondali. Mentre i tecnici dell'intelligence intervenivano a riva, prima che i tubi si gettassero in acqua. L'avvento dei social media ha rivoluzionato il sistema di spionaggio, integrando le tecniche subacquee (*down-*

stream) con quelle terrestri (*upstream*), trasformando definitivamente la Rete nel dominio statunitense.

Sul piano del software, Washington ha cominciato a finanziare gli sviluppatori degli algoritmi a partire dagli anni Novanta, quando si è convinta di voler sfruttare Internet in funzione esterna. Ne sono germinati gli attuali colossi high tech, capaci di fornire agli esseri umani la possibilità di comunicare attraverso la messaggistica istantanea.

Così oggi miliardi di cittadini – attraverso post, mail, blog – affidano i loro pensieri più intimi alle società della californiana Silicon Valley, più Microsoft e Amazon che hanno sede a Seattle. Di fatto l'80% della popolazione connessa nel pianeta, che offre agli americani la più grande quantità di informazioni della storia. «Basti pensare che dalla comparsa della civiltà al 2003 sono stati creati dati per cinque exabyte e che adesso produciamo la stessa quantità in appena due giorni»², ha spiegato l'ex amministratore delegato di Google (Alphabet), Eric Schmidt.

Il potere di motori di ricerca e social statunitensi è nei dati. Google, Yahoo! e Bing controllano insieme il 98% delle ricerche realizzate a livello mondiale (soltanto Google ne è destinatario per il 92%). Facebook, Twitter, YouTube, Pinterest, Instagram assorbono il 96% degli iscritti alle reti sociali (soltanto Facebook vale il 66% del totale, per un corrispettivo di 2,2 miliardi di utenti)³. La loro influenza nei paesi satelliti degli Stati Uniti risulta addirittura impressionante. Google gestisce il 90% delle ricerche realizzate in Italia, l'86% in Francia, l'82% in Gran Bretagna, il 70% in Giappone. Addirittura il 94% in India⁴. Facebook vanta 131 milioni di utenti attivi in Indonesia, 129 milioni in Brasile, 60 milioni in Vietnam, 40 milioni nel Regno Unito. Fino a 295 milioni in India⁵.

A fornire spontaneamente informazioni ai siti americani sono anche i cittadini dei governi rivali, da tempo impegnati a bloccare l'accesso al loro territorio e a sviluppare omologhi degli originali, eppure costretti ad accettare l'intrusione delle aziende straniere. Google è destinatario dell'87% delle ricerche realizzate a Hong Kong, del 40% di quelle effettuate in Russia, del 6% nell'intero territorio cinese⁶. Così Facebook raccoglie il 75% degli abitanti di Hong Kong, il 51% degli utenti turchi, il 21% di quelli russi (pressoché lo stesso numero del corrispettivo locale, VKontakte)⁷. Senza contare l'accesso clandestino ai social statunitensi che realizzano i cittadini di paesi in cui questi sono formalmente banditi. Come in Iran, dove Twitter risulta assai frequentato attraverso diffusi sistemi di mistificazione⁸.

2. Citato in B. UPBIN, «The Web Is Much Bigger (And Smaller) Than You Think», *Forbes*, 24/4/2012.

3. Cfr. *Statcounter, Search Engine and Social Media Stats Worldwide*, settembre 2018, goo.gl/KX739Q

4. Cfr. *Statista: Share of Desktop Search Traffic Originating from Google in Selected Countries*, giugno 2018, goo.gl/Wg3qXn

5. Cfr. *Statista: Leading Countries Based on Number of Facebook Users*, ottobre 2018, goo.gl/ozaVkh

6. Cfr. *Statista, Share of Desktop Search Traffic Originating from Google in Selected Countries*, cit.

7. Cfr. *Statcounter, Social Media Stats Worldwide*, settembre 2018. goo.gl/8M3Ha9

8. Cfr. G. ESFANDIARI, «Iranian Politicians Who Use Twitter Despite State Ban», *Radio Free Europe*, 28/8/2017.

Come previsto dalla legge americana, la Silicon Valley garantisce all'intelligence nazionale il libero accesso ai dati. I server sono presenti esclusivamente sul suolo statunitense, soggetti a rogatoria internazionale qualora Stati stranieri volessero accedervi, sottoposti alla volontà delle istituzioni federali. Come svelato nel 2013 dall'ex *contractor* dell'Nsa Edward Snowden, si tratta di un sistema (Prism e succedanei) in funzione dal 2007, cui almeno inizialmente hanno aderito Microsoft, Apple, Google, YouTube, Yahoo!, Facebook, Skype, Aol e Paltalk. Confermato nel tempo, nonostante le blande leggi adottate in materia dal Congresso per placare lo sconcerto dell'opinione pubblica – compreso lo Usa Freedom Act del 2015, che tuttora riconosce alle autorità federali l'assoluta discrezione nello stabilire chi spiare e perché.

Tramite i dati, gli analisti americani sono convinti di poter conoscere i cittadini stranieri meglio dei loro governanti, dunque di anticiparne le tendenze politiche, le reazioni a impulsi specifici. Sicuri di poter innescare rivolte di piazza, qualora gli utenti si mostrassero pronti al cambiamento. Di controllare da remoto quanto avviene nel pianeta. Probabilmente un'illusione, almeno finché i dati non saranno vagliati attraverso le categorie della geopolitica umana⁹. Eppure una miniera potenzialmente decisiva, cui la superpotenza non intende rinunciare. Simbolo stesso della supremazia di Washington sulle società private, costrette a conformarsi alla strategia nazionale, ad anteporre gli interessi del paese al proprio profitto. Per ragioni storiche e antropologiche, intrinseche al sentire americano.

3. Tra gli ameni pregiudizi del nostro tempo vi è quello che stabilisce l'autonomia delle multinazionali rispetto ai governi. *Boutade* distillata Oltreoceano a esclusivo uso esterno, accolta fideisticamente in società post-storiche informate dal primato economicistico, perfettamente sconosciuta nel contesto statunitense. Soprattutto nel settore informatico, dipendente dallo Stato per la propria tecnologia, profondamente immerso nella società anglosassone, da sempre ancillare all'azione del paese. Anzitutto, a determinare la fragilità della Silicon Valley è la consapevolezza di non aver inventato la tecnologia di cui si serve. Qualsiasi prodotto e servizio offerto nell'high tech ha avuto origine al Pentagono, non in California.

Internet fu inventato dall'Arpanet, il network dell'antesignano dell'attuale Darpa, il potentissimo ufficio per l'innovazione della Difesa. L'obiettivo era disporre di un sistema di comunicazione interna. Il microprocessore, il cuore di ogni computer e di ogni smartphone, fu creato su iniziativa dello Stato federale che necessitava di un dispositivo leggero per telecomandare missili, aerei e altri sistemi. Fu provato inizialmente sui caccia F-14, quindi sui sottomarini nucleari, poi sui missili balistici intercontinentali. Così il telefono cellulare fu realizzazione congiunta della General Dynamics (in passato Gte) e dell'Esercito statunitense, alla ricerca di un telefono portatile da usare in battaglia. Fu impiegato per la prima volta dal generale Norman Schwarzkopf durante la campagna per il Kuwait. Perfino Siri, il sistema di ricono-

scimento vocale installato su ogni iPhone, è stato ideato dal centro di ricerca Sri, un progetto finanziato dalle Forze armate.

Del resto, per ragioni di calcolo del rischio, le aziende private non possono spendere in innovazione quanto lo Stato federale. Attraverso specifici uffici e società di venture capital, nel corso degli anni il Pentagono, la Cia e l'Nsa hanno finanziato, direttamente o indirettamente, la nascita di Microsoft, Facebook, Google, Paypal, Yahoo!, Amazon, Twitter, YouTube. Ancora oggi il ministero della Difesa spende in sviluppo e ricerca circa 72 miliardi di dollari, più del doppio della cifra cumulata di Apple, Intel e Google. Anziché essere alla testa di una rivoluzione tecnologica, i giganti della Silicon Valley si sono limitati a riadattare per uso civile strumenti di cui non possiedono il brevetto. Con la subordinazione allo Stato federale che questo comporta e il fisiologico terrore d'essere estromessi dal mercato da chi realizzerà concretamente la prossima invenzione. Come ammesso da Peter Thiel, co-fondatore di Paypal e di Palantir, tra i più lucidi osservatori del settore, «la strada delle invenzioni non è infinita. Tanto vale imboccare percorsi alternativi»¹⁰.

Per estrazione etnica e di genere della loro classe dirigente, le grandi aziende informatiche restano profondamente statunitensi. Nonostante si vendano come patrimonio dell'umanità, nonostante abbiano sede nella spuria California. L'intero management di Facebook è di chiara origine tedesca, dunque appartenente al primo ceppo etnico della nazione. Si tratta del fondatore e amministratore delegato Mark Zuckerberg; del direttore operativo, Sheryl Sandberg; del direttore finanziario, David Wehner; del direttore tecnico, Mike Schroepfer. Così sono di discendenza teutonica tutti gli ideatori di Tesla: Elon Musk, Martin Eberhard, Marc Tarpenning, J. B. Straubel.

Lo stesso vale per l'ad di Amazon, Jeff Bezos (vero cognome, Jorgensen); per il suo direttore tecnico, Werner Vogels; per l'ad di Paypal, Dan Schulman; per il responsabile tecnico di Space X, Tom Mueller; per l'ad di Palantir, Alex Karp; per lo stesso Peter Thiel, nato a Francoforte sul Meno. Ancora, erano di provenienza germanica lo storico fondatore di Apple, Steve Jobs (all'anagrafe Jandali Schieble) e l'ex amministratore delegato di Google, Eric Schmidt.

Secondo rapporti ufficiali diffusi l'anno scorso da Apple e Google, rispettivamente il 57% e il 56% dei loro posti di lavoro sono occupati da bianchi, contro il 21% e il 29% detenuto da asiatici, il 13% e il 4% da ispanici e il 9% e il 2% da neri. Con un dato che nel settore high-tech segnala il 65% di assunti anglosassoni¹¹, perfino più alto della media nazionale (61%). In una nazione culturalmente omogenea come gli Stati Uniti, tanta appartenenza al gruppo dominante si traduce in spontanea aderenza al pensiero collettivo.

Peraltro i giganti della Rete sono consapevoli d'essere soggetti ai capricci di Washington. Qualora volesse, il Congresso potrebbe approvare stringenti norme

10. Citato in P. THIEL, B. MASTERS, *Zero to One: Notes on Startups, or How to Build the Future*, Redfern 2014, Currency.

11. Cfr. L. IOANNU, «Silicon Valley's Achilles' Heel Threatens to Topple Its Supremacy in Innovation», *Cnbc*, 20/6/2018.

antitrust, oppure sulla privacy, che di fatto impedirebbero alle aziende della Silicon Valley (e di Seattle) di sopravvivere. Vero, senatori e deputati non comprendono come funziona tecnicamente Internet, ma hanno i mezzi per sbriciolarlo in molteplici centri di potere, di azzerarne i principali bacini di potere. Come capitato in passato attraverso lo Sherman Antitrust Act (1890), utilizzato dalle amministrazioni Roosevelt e Taft soprattutto contro la Standard Oil Company e l'American Tobacco Company.

Per questo dalla sua nascita il comparto informatico intrattiene solidi rapporti con la Casa Bianca e con il parlamento. Da quando nel 1993 l'allora amministratore delegato di Apple, John Scully, si incontrò con il presidente Bill Clinton e il suo vice Al Gore. Inaugurando una consuetudine che ha attraversato molteplici amministrazioni. Fino al teso vertice del dicembre 2016 tra l'attuale presidente degli Stati Uniti, Eric Schmidt e Alex Karp.

Ancora più rilevante, nel tentativo di comprarsi la benevolenza di deputati e senatori, negli anni la Silicon Valley è divenuta il settore che maggiormente versa in lobbying al congresso. Nel 2017 Google, Facebook, Microsoft, Apple e Amazon hanno speso 56,8 milioni di dollari¹², più del doppio di quanto sborsato da Wall Street, storicamente in testa a tale classifica. Nel 2018 soltanto Google (Alphabet) ha investito 18,3 milioni, seguito da Amazon con 10,6 milioni e da Facebook con 9,7 milioni¹³. Dati che palesano la netta preminenza delle istituzioni sul resto. A dispetto della retorica indipendentista delle multinazionali, incentivata dalla stessa amministrazione federale per poter agire surrettiziamente in contesti stranieri ed evitare di rispondere direttamente di quanto capita in teatri sensibili.

Mentre da alcuni anni Pentagono e Cia hanno aperto nella valle californiana proprie filiali – rispettivamente DIUx a Mountain View e In-Q-Tel a Palo Alto – con l'obiettivo di sfruttare e incentivare eventuali miglioramenti della tecnologia realizzati in loco. Nonché impedire ad aziende e start-up di perseguire interessi economici contrari a quelli della nazione. A tal fine il Pentagono dispone perfino di un suo ambasciatore, formalmente il presidente della Defense Innovation Unit, incaricato di imporre la propria visione al contesto. Si tratta di Michael Brown (vero cognome, Braun), portatore di una visione profondamente anticinese, intenzionato a conservare il gap industriale ai danni di Pechino e di servirsi a tal fine di Giappone e Germania, gli alleati maggiormente capaci sul piano tecnico. Non a caso Brown è stato coautore del rapporto Diux che informa l'attuale offensiva dell'amministrazione Trump contro lo sviluppo tecnologico della Repubblica Popolare. Prodromi del prossimo scontro con l'antagonista asiatico. In vista del quale, la Silicon Valley va necessariamente mantenuta nello spazio di manovra conferitole.

4. Nella dimensione terrestre, come in quella virtuale, gli Stati Uniti restano in posizione dominante. Benché il pianeta ci appaia sull'orlo del caos e l'ordine internazionale decaduto, gli sfidanti della superpotenza sono tuttora costretti a combat-

tere battaglie di retroguardia, per non sprofondare. La Russia dispone di propri social network con cui (parzialmente) schermarsi dall'infiltrazione straniera, ma i suoi troll sono costretti a intervenire sulle piattaforme d'Oltreoceano per realizzare la *dezinformacija*. Altrimenti il loro operato sarebbe semplicemente ininfluente. Così la Cina, che pure rimane la nazione maggiormente immune dall'ingerenza altrui, dopo aver incentivato negli anni la nascita di omologhi delle aziende statunitensi, non riesce a esportare i propri social network e motori di ricerca all'estero – Baidu controlla appena l'1,37% delle ricerche mondiali, WeChat tocca il 26% della messaggistica ma con una presenza rilevante soltanto nel paese di origine, a Taiwan e in Malaysia¹⁴. Piuttosto è costretta a utilizzare Internet per spiare i propri cittadini, anziché quelli degli altri.

Situazione sfavorevole che in questa fase l'Impero del Centro prova a rovesciare – la Russia non ne ha neppure l'ambizione. Non solo lanciando lo spettacolare progetto delle nuove vie della seta, tentativo di sottrarsi allo strapotere marittimo degli Stati Uniti. Provando a ridurre lo iato esistente anche nel dominio informatico, dove è più semplice intervenire che nella dimensione militare, perché meno dispendioso in termini di costi e conoscenza. Soprattutto attraverso ingenti investimenti nello sviluppo dell'intelligenza artificiale e con l'imposizione delle proprie regole, in materia di censura e cessione dei dati, alle società straniere che ne vogliono penetrare lo smisurato mercato. Obiettivo ultimo è distruggere l'egemonia universale di Washington, ricavandosi una propria sfera di influenza, virtuale e reale. Legando a sé quei paesi che vorranno abbracciare l'intelligenza artificiale di sua produzione, costringendoli ad accoglierla in esclusiva, a rifiutare quella americana. Oppure ponendoli al cospetto del dilemma di dover duplicare le piattaforme, con l'enorme danno in termini di costi che questo comporterebbe.

Consapevole della manovra in atto, Washington intende impedire a Pechino di dotarsi della tecnologia necessaria a realizzare tanto proposito, ad azzerare lo scarto che esiste tra i due paesi, a frastagliare la Rete. Sventando qualsiasi trasferimento di competenza, nonché l'acquisizione da parte cinese di società statunitensi dotate di specifica expertise. Nella convinzione che, senza drenare know-how dall'estero, la Repubblica Popolare non possa inficiare la primazia degli Stati Uniti. Perché priva degli strumenti necessari per attirare le altre nazioni, specie se a queste chiedesse di rompere con Washington.

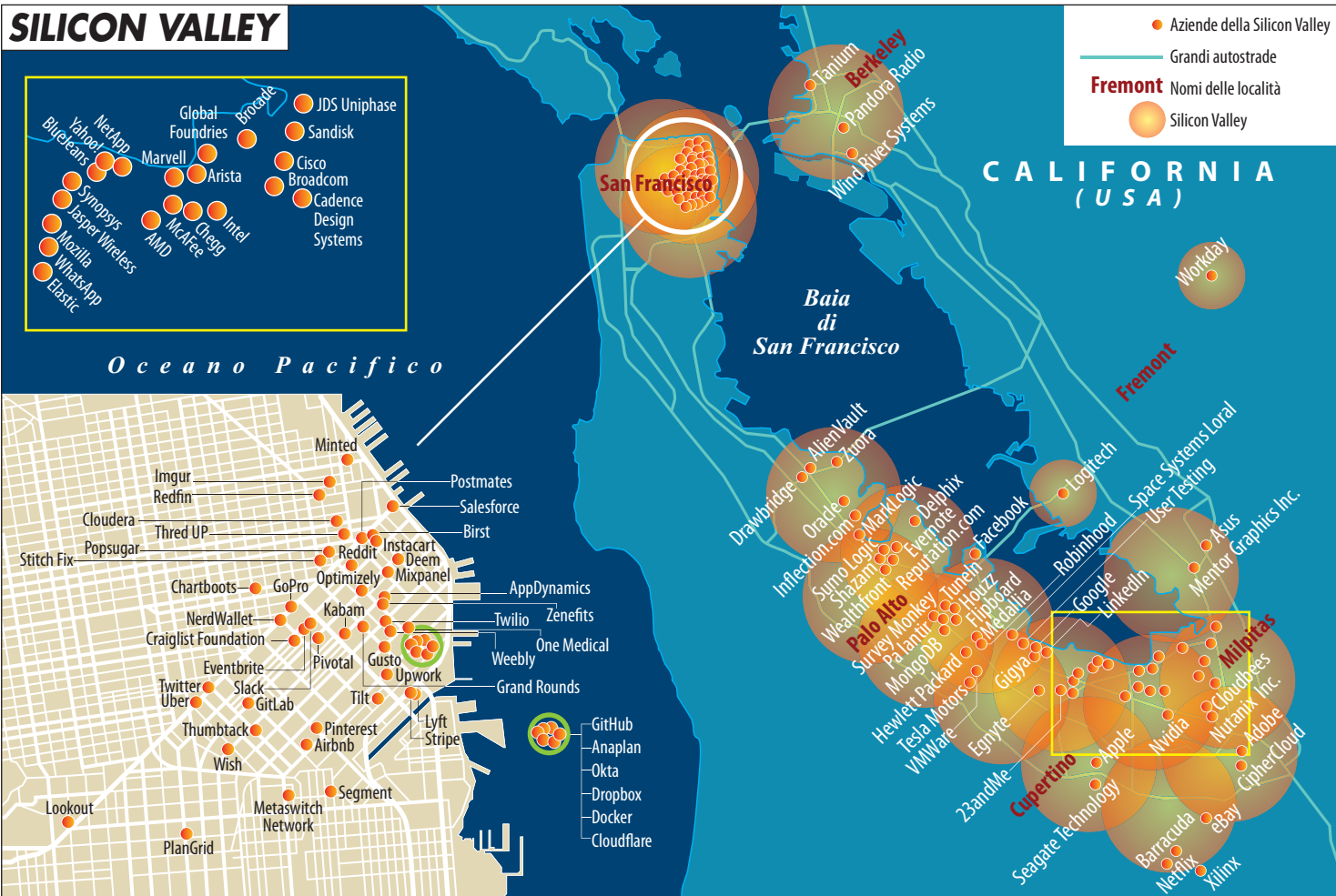
Da tale approccio sono scattati i dazi imposti dall'amministrazione Trump alla Repubblica Popolare, disegnati per colpire le aziende cinesi che producono macchinari e strumenti legati allo sviluppo tecnico. Per la medesima ragione, nel nuovo Nafta sono state inserite clausole che vietano ai partecipanti di siglare un'intesa con Pechino. Pena la rescissione del trattato da parte statunitense. Quindi in questa fase Washington interviene massicciamente sul ruolo che potrebbe giocare la Silicon Valley. Nel timore che, attirati dalle possibilità di guadagno offerte dal mercato cinese, i magnati informatici possano deragliare dall'azione statunitense. Illudendo-

14. Cfr. *Statscounter, Search Engine Market Share Worldwide*, settembre 2018.

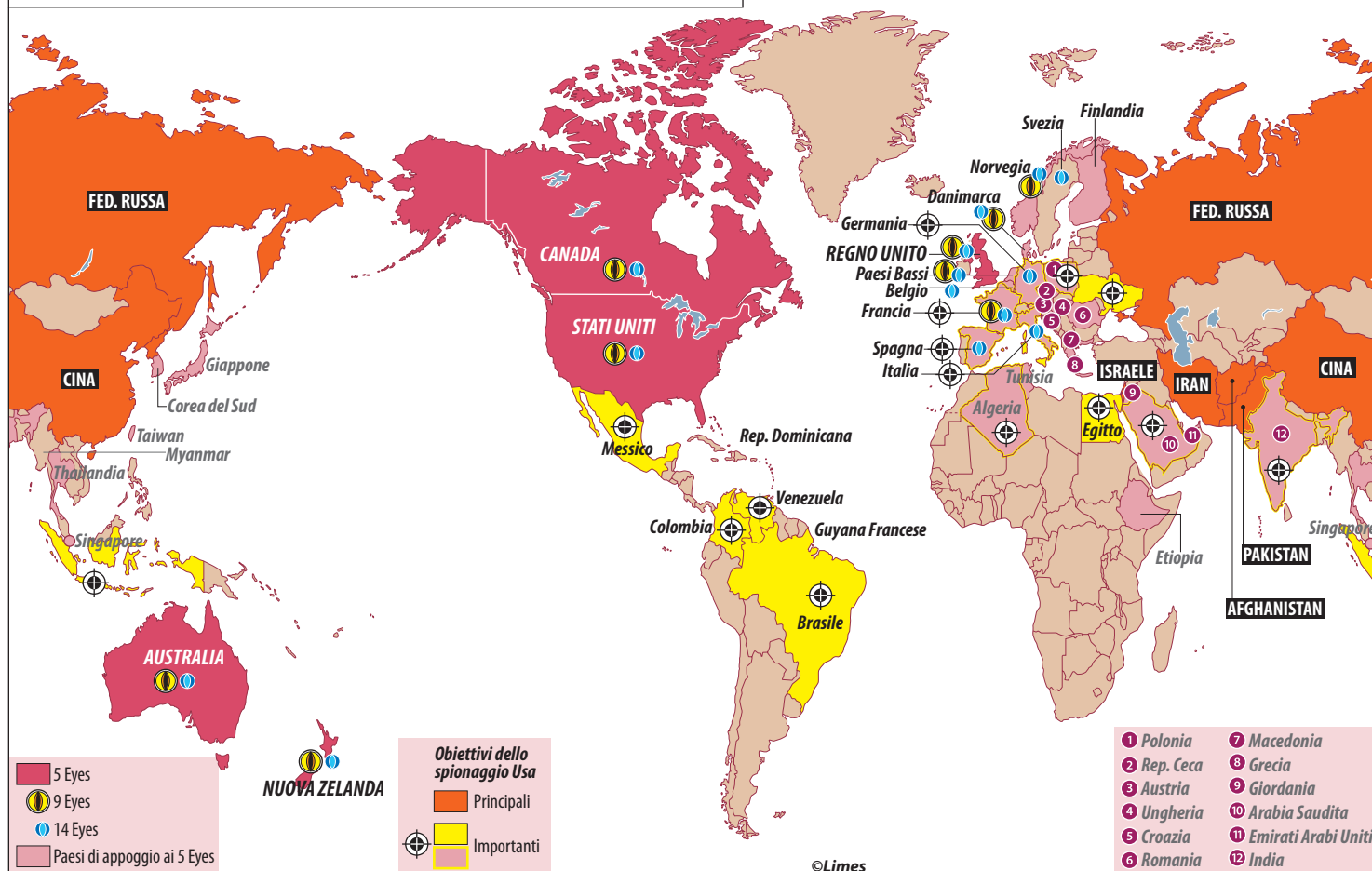
LA SFIDA DELL'INTELLIGENZA ARTIFICIALE



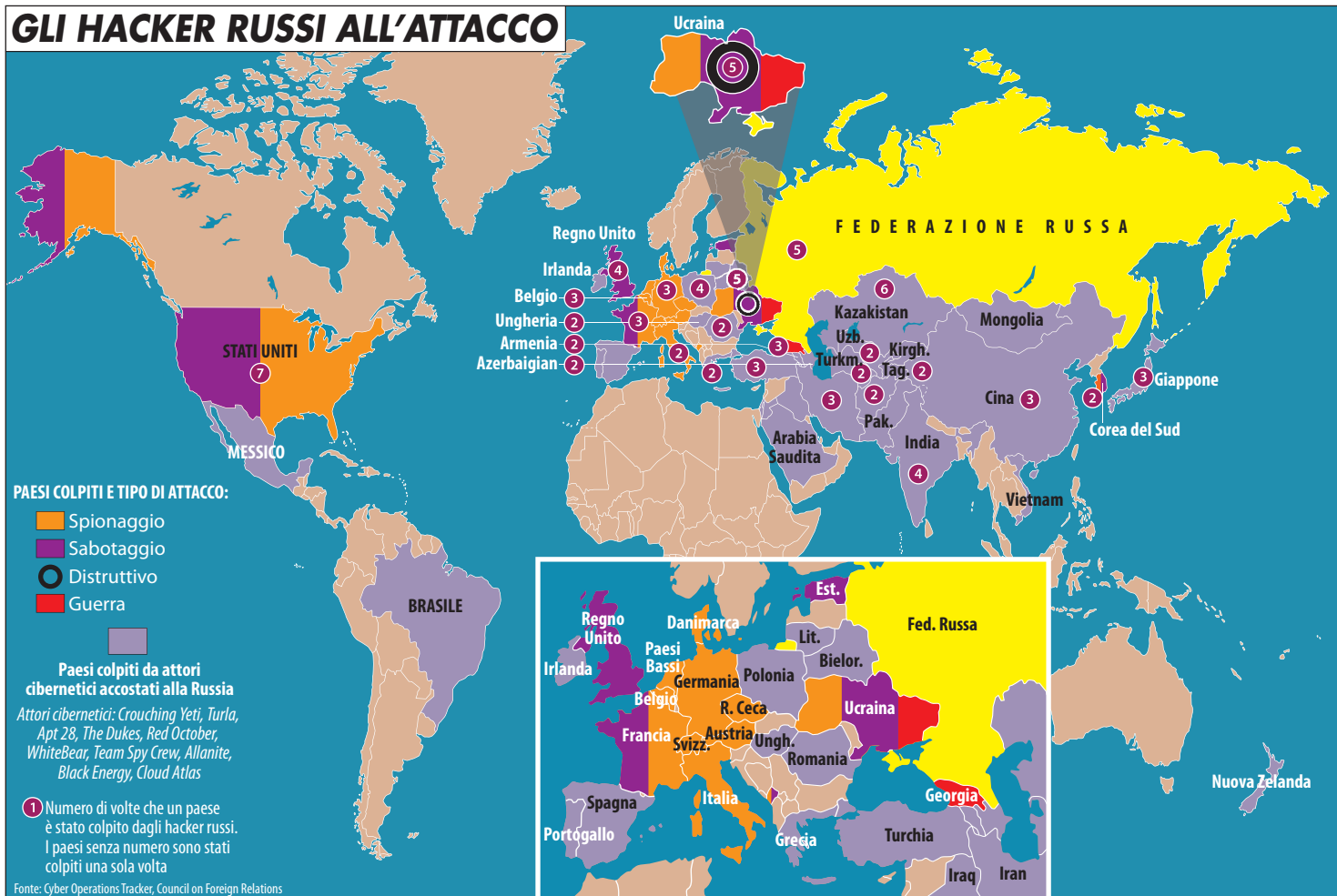
SILICON VALLEY



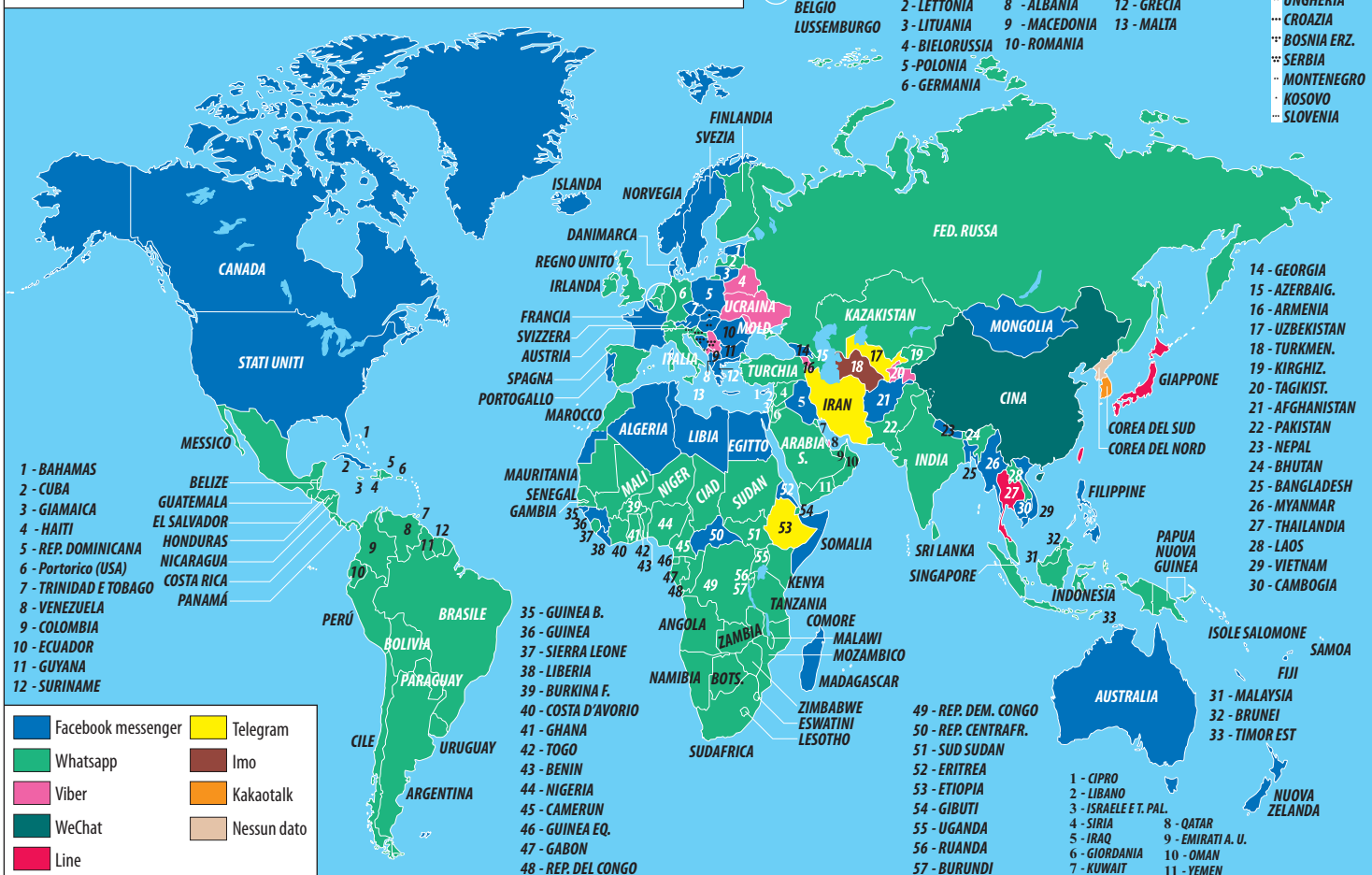
CON CHI E CONTRO CHI SPIANO GLI USA



GLI HACKER RUSSI ALL'ATTACCO



PRIME APP DI MESSAGGISTICA PER PAESE



Fonte: Similarweb gennaio 2018, dati basati sulla classifica di Google Play Store, per paese, 2017

si di poter conciliare profitto e interesse nazionale. Fino a partecipare, involontariamente, al disegno secessionista cinese.

Di qui la plateale avversione di Trump alla valle californiana, più volte segnalata già durante la campagna presidenziale. «Si tratta di aziende che non hanno mai prodotto introiti reali, eppure sono valutate miliardi. Rischiano seriamente di scoppiare»¹⁵, aveva ammonito nel maggio del 2016. Ostilità motivata non soltanto dall'inclinazione sinistrorsa del contesto pacifico e dal noto analfabetismo informatico dell'oligarca newyorkese. Esplicito è l'obiettivo di rammentare ai suoi interlocutori la necessità di aderire all'azione del governo. Specie in seguito a previsioni apocalittiche e atteggiamenti considerati troppo simpatetici nei confronti della Cina da parte dei leader dell'high tech. Dopo che Eric Schmidt ha preannunciato per il 2028 una Rete divisa in due, tra una parte a guida americana e una a guida cinese¹⁶. E dopo che Mark Zuckerberg s'è lasciato fotografare con il primo volume di *Il governo della Cina*, tomo monumentale che raccoglie i discorsi di Xi Jinping.

Proprio Zuckerberg lo scorso aprile ha sperimentato la potenziale furia di Washington. Quando è stato costretto a chiedere drammaticamente perdono al Senato americano per aver venduto dati alla società britannica Cambridge Analytica, che a sua volta li avrebbe girati a compratori russi, velleitariamente impegnati a influenzare il processo politico d'Oltreoceano. «Gli accordi che proponete agli utenti fanno schifo (...) dovete fare maggiore attenzione»¹⁷, gli ha urlato contro il senatore della Louisiana, John Neely Kennedy. Tradotto: la Silicon Valley non può fare intelligenza con il nemico. Di qualsiasi nazionalità sia.

In piena sindrome cinese, l'attenzione dell'amministrazione federale nei confronti del comparto informatico è sensibilmente aumentata. Esercitata attraverso un misto di lusinghe e minacce. Per cui agli insulti è seguita la riforma fiscale approvata dal Congresso, di cui beneficiano largamente proprio le aziende cibernetiche (solo Apple ha ottenuto 14 miliardi di dollari dagli sgravi fiscali). Quindi i lucrosi contratti sottoscritti da Palantir e Amazon, società scelte perché ritenute ortodosse in termini geopolitici. A convincere Washington è stato proprio l'afflato anticinese di Peter Thiel, certo che «la Repubblica Popolare non riuscirà mai a raggiungere gli Stati Uniti»¹⁸. E la delusione subita da Amazon, cui è stata precluso l'ingresso nel territorio cinese dal governo comunista, intenzionato a prediligere l'autoctono Alibaba.

Specializzata nell'analisi dei dati, negli ultimi mesi Palantir ha ottenuto un appalto da 876 milioni di dollari per ricostruire il sistema di intelligence informatica delle Forze armate. Mentre Amazon, dopo aver siglato un contratto analogo con la Cia, ora è favorita per realizzare il *cloud* interno al Pentagono, per un totale di 10 miliardi di dollari.

15. Citato in H. SOMVERVILLE, «Silicon Valley Mocks Trump over His Tech Bubble Warning», *Reuters*, 18/5/2016.

16. Citato in I. Hamilton, «Google's Ex-CEO Eric Schmidt Says the Internet Will Split in Two by 2028», *Business Insider*, 21/9/2018.

17. Citato in C. AIELLO, «Senator to Zuckerberg: "Your User Agreement Sucks"», *Cnbc*, 10/4/2018.

18. Cfr. P. THIEL, B. MASTERS, *op. cit.*

I maggiori sospetti dell'amministrazione federale si concentrano su Google (Alphabet) e Facebook. Non a caso nel 2017 Schmidt ha lasciato la guida della multinazionale di Mountain View, perché portatore di una visione del mondo in contrasto con lo spirito del tempo. Ad alimentare lo scrutinio ai loro danni la volontà di rientrare in territorio cinese. Segnalata per Google dalla partecipazione nel progetto di motore di ricerca *Dragonfly*, con cui Pechino sperimenta nuovi strumenti di censura. E per Facebook dai test condotti in loco per la creazione di una applicazione di condivisione delle foto.

Colti sul vivo, adesso gli apparati segnalano ai due colossi quale siano i termini per ottenere luce verde per il ritorno in Cina. Ovvero, consegnare a Washington informazioni decisive sulla popolazione cinese, su quanto accade nel ventre del rivale. Senza accettare interamente la censura imposta da Pechino, senza acconsentire all'utilizzo altrui dei propri server, senza partecipare alla definitiva creazione di un Internet in salsa rossa. Acrobazia di complessa riuscita, su cui lo Stato profondo non transige. Destinata nei prossimi anni a informare la tattica americana. Con l'obiettivo di mantenere subordinata la Repubblica Popolare, di impedire che nell'impero informatico si creino feudi indipendenti.

5. Storicamente ogni egemone dispone di un notevole vantaggio tecnologico. I romani erano superiori al resto nell'architettura e nell'arte militare, gli arabi nell'agricoltura e nella matematica, gli inglesi nella navigazione e nell'industria. La tecnologia non è mai fondamento dell'egemonia, non può supplire all'assenza di diffuse capacità antropologiche. Eppure è indispensabile per aumentare il distacco dagli avversari, per corroborare uno specifico passaggio temporale. Da decenni gli Stati Uniti dispongono di superiorità informatica, prima capace di condurre l'Unione Sovietica alla consunzione, poi di tradursi nella dimensione virtuale della primazia, quindi nel maggior contributo tecnico fornito alla storia.

Impossibilitata a competere sul terreno militare, la Cina prova a sfidare la superpotenza proprio in ambito tecnologico, laddove il governo centrale può fissare unilateralmente l'obiettivo e la cospicua liquidità per perseguirlo. Nella speranza di realizzare la svolta, di capovolgere la propria condizione di isolamento, di distruggere l'universalità altrui. Finendo per innescare la reazione di Washington, compresa quella della Casa Bianca. Per cui, alle prese con tanto attacco, Trump ha abbandonato lo sbandierato isolazionismo per adottare un afflato eminentemente estrovertito, per scagliarsi contro chi vuole ridurre la grandezza geografica dell'autorità statunitense. Fino a utilizzare il protezionismo per colpire la Repubblica Popolare, fino a prodigarsi nel firmare accordi multilaterali di libero scambio, in barba a quanto promesso in campagna elettorale. Mentre gli apparati impongono alla Silicon Valley le mosse da adottare, così da evitare incontrollabili scatti in avanti che danneggino la posizione dominante del paese. Affinché l'Internet globale continui a raddoppiare la profondità della *pax americana*, affinché resti integro in ogni sua declinazione. Dalle rotte marittime ai satelliti, dai cavi sottomarini alle nuvole di memorie, dai chip agli organi vitali degli esseri umani. Volto trascendente dell'impero statunitense.

SE VINCONO GLI ALGORITMI PERDE L'UMANITÀ

di Frank PASQUALE

I giganti della tecnologia progettano un mondo nel quale le macchine sostituiranno il fattore umano. I compromessi inaccettabili di Facebook e il transumanesimo del guru di Google. Il cortocircuito tra riservatezza e libertà. Diventeremo un flusso di dati?



1. QUANDO COMINCI AI SCRIVERE DI MOTORI di ricerca ero entusiasta di questa nuova tecnologia. In uno dei miei primi articoli sollecitai i tribunali a rendere meno severe le norme sulla protezione del diritto d'autore per fare in modo che aziende come Google potessero organizzare meglio libri, film, giornali e altro ancora¹. All'epoca ero convinto che il sovraccarico di informazioni costituisse una conseguenza inintenzionale negativa del successo della legge sul diritto d'autore nell'incentivare la produzione e la distribuzione dell'espressione individuale. Se i tribunali avessero conferito ai proprietari il diritto di opporre il veto al tentativo dei classificatori di catalogare i contenuti da essi prodotti, non avrebbero fatto altro che esacerbare il problema.

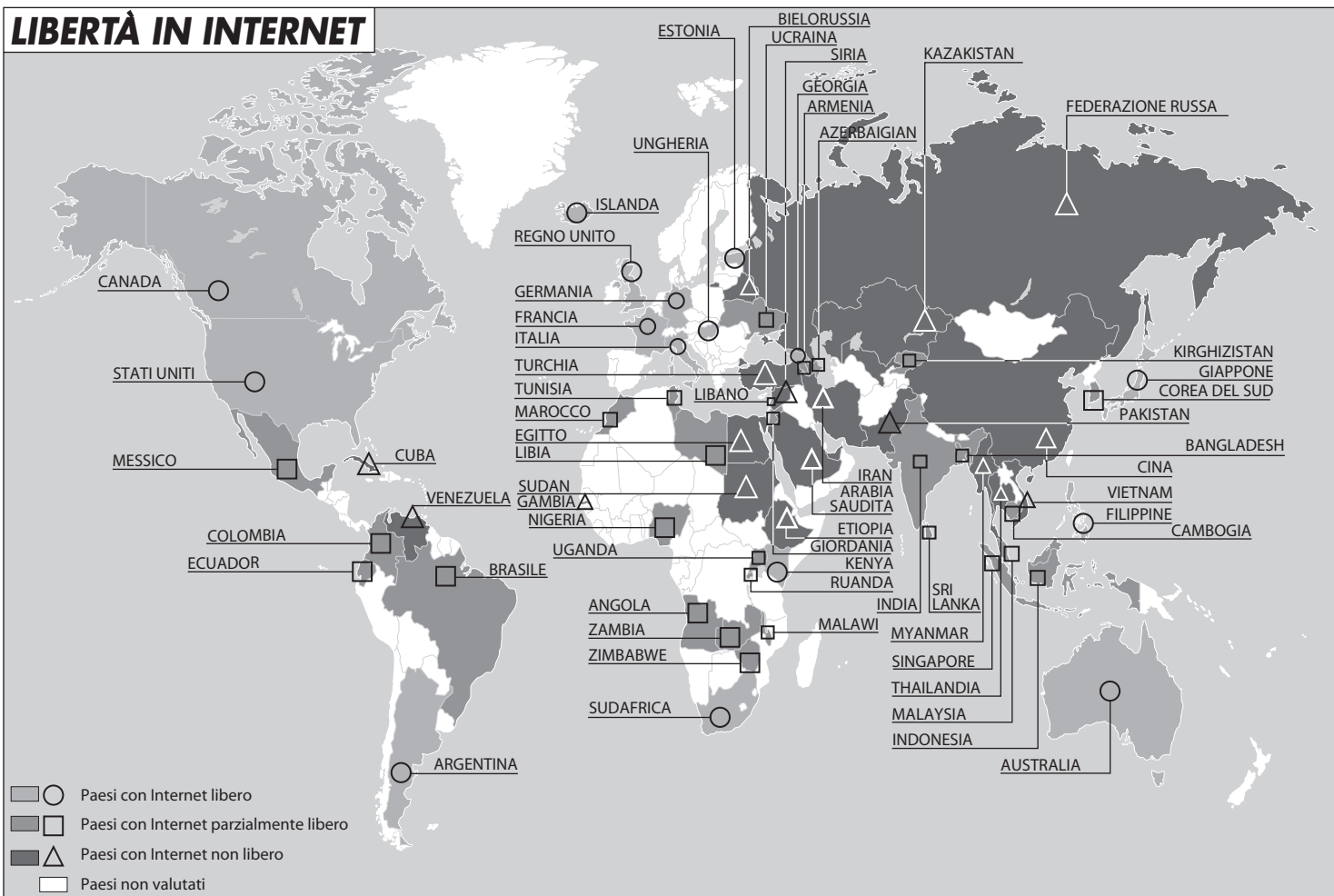
Quello che non mi aspettavo era il modo spietato in cui Google avrebbe usato questa libertà per avere la meglio nella battaglia contro gli editori e i fornitori di contenuti sui termini d'accesso al lavoro creativo. Non avevo previsto neanche come Amazon e Apple avrebbero usato il loro potere per mettere in ginocchio le industrie creative. In parte per espiare le mie precedenti iniziative, di recente ho promosso alcune proposte per riformare le leggi antitrust in modo da permettere ai media di contrattare pagamenti più equi con i grandi intermediari². Nel frattempo, ho anche individuato molti modi in cui alcune leggi, o interpretazioni delle stesse, hanno concesso alle grandi aziende del settore tecnologico vantaggi ingiusti nei confronti delle altre imprese.

Sulle piattaforme dei giganti della tecnologia sono inoltre emerse tendenze preoccupanti in merito alla soppressione della libertà d'espressione. Tali piatta-

1. F. PASQUALE, «Copyright in an Era of Information Overload: Toward the Privileging of Categorizers», *Vanderbilt Law Review*, 2007, Seton Hall Public Law Research Paper n. 888410, goo.gl/2JkWCq

2. D. CICILLINE, «Cicilline Introduces Journalism Competition and Preservation Act», *cicilline.house.gov*, 7/3/2018, goo.gl/Mz1F1Z

LIBERTÀ IN INTERNET



Fonte: Freedom House, 2017

forme possono infatti emarginare (o bloccare del tutto) connessioni potenziali tra chi riceve e chi fornisce informazioni. Si presentano dunque seri problemi relativi alla protezione dei consumatori, dal momento che le piattaforme che vengono commercializzate come aperte, complete e imparziali sono in realtà chiuse, incomplete e autoreferenziali. Le piattaforme incriminate rispondono a queste accuse asserendo il proprio diritto a creare l'ambiente informativo che più gli aggrada o abiurando ogni responsabilità, rivendicando di riflettere meramente i desideri e le preferenze dei suoi utenti. Tutto ciò porta a quella che ho definito una «comoda crisi d'identità»³. Le grandi aziende del comparto tecnologico sostengono che ciò che producono (soprattutto flussi di notizie e risultati di ricerca) è protetto dalla libertà d'espressione quando vogliono far valere quest'ultimo diritto. Ma quando vengono accusate di disseminare contenuti pirata, immagini offensive o truffe pericolosamente ingannevoli nel campo della medicina, affermano di essere unicamente i canali, le «tubature» di un'infrastruttura comunicativa.

Il problema principale, in questo contesto, è che la vecchia classificazione dei media non ha più senso nell'era digitale. Le grandi piattaforme online assumono la forma tanto di canali di comunicazione quanto di fornitori di contenuti. Per disinnescare i pericoli gemelli del monopolio e della sorveglianza totale, che minacciano la libertà d'espressione, sono necessarie regole per ognuna delle due dimensioni della questione.

Un altro problema enorme posto dalle grandi aziende del comparto tecnologico è l'opportunistica combinazione di riservatezza commerciale e protezione della libertà d'espressione. Quando le persone si insospettiscono per risultati di ricerca tendenziosi o per il modo in cui le notizie rimbalzano sui social network, i giganti del settore tendono a rispondere: «Scusate, i metodi che usiamo per classificare e valutare le informazioni sono segreti commerciali»⁴. L'unico modo con cui si può ottenere accesso a questi metodi di classificazione e valutazione è intentare una causa per diffamazione, illecito, concorrenza sleale o per la tutela dei diritti dei consumatori. A quel punto, le aziende del settore tecnologico di solito sostengono che «ciò che produciamo rientra nella nostra libertà d'espressione, abbiamo diritto di dirlo, senza conseguenze legali». Tutto quello che finisce nelle loro scatole nere, dunque, è un segreto commerciale e tutto quello che viene pubblicato è protetto dalla libertà d'espressione. Il risultato è la ricetta perfetta per sfuggire alla responsabilità giuridica.

2. Nei mercati digitali la specializzazione eclissa la visione d'insieme. Come in ogni altro campo, la legge può soccombere di fronte a tale dinamica. Nel caso delle società dell'Internet, ad esempio, gli avvocati specializzati nel diritto delle

3. F. PASQUALE, «Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power», 17 *Theoretical Inquiries in Law* 487 (2016), University of Maryland Legal Studies Research Paper n. 24-2016, goo.gl/gK4rxL.

4. F. PASQUALE, «Search, Speech, and Secrecy», *Yale Law & Policy Review*, 2010, goo.gl/ZnQytQ; ID., «The Troubling Consequences of Trade Secrecy Protections for Search Results», *Handbook of Trade Secrecy Research*, 2010.

tecnologie si limitano spesso a dire: «Google e Facebook dovrebbero vincere le cause più importanti sul diritto d'autore, quelle successive sui marchi commerciali, le cause sulla concorrenza, dovrebbero godere di alcune immunità in materia di libertà d'espressione e non dovrebbero essere considerate "agenzie di rilevazione dei consumatori" nell'ambito delle leggi sulla privacy pertinenti». Questi legali possono anche avere ragione in merito a ogni singolo caso, ma che cosa accade quando una massa di casi simili tra di loro si combina con effetti di rete che conferiscono a un pugno di aziende un potere incredibile sulle informazioni a nostra disposizione e persino sulla nostra interpretazione delle stesse? È necessario sviluppare nuove forme di concorrenza o nuove regole affinché chi beneficia di questi appigli giuridici non usi il suo potere per controllare fette sempre più grandi dell'economia. Lo stesso principio che ha portato a una separazione tra banche commerciali e banche d'investimento negli Stati Uniti dovrebbe indurre i legislatori americani a considerare anche una separazione della rete sociale dalla sezione notizie (nel caso di Facebook) o delle piattaforme dalla vendita di prodotti (nel caso di Amazon e Google).

Sorprendentemente, molti tecnocrati americani alla guida delle agenzie coinvolte sono andati nella direzione esattamente opposta per almeno un decennio. Agenzie che avrebbero dovuto proteggere i mercati dall'interferenza dei giganti del comparto tecnologico si sono invece allineate a essi, presentando efficacemente il loro dominio come una soluzione alla stagnazione economica, invece che come causa della stessa. La Commissione federale per il commercio degli Stati Uniti si è espressa a favore di Google in una disputa tra l'azienda di Mountain View e gli inserzionisti e a favore di Uber quando gli autisti intendevano negoziare collettivamente. Queste decisioni possono essere spiegate solo facendo i conti con la terza dimensione del potere dei giganti della tecnologia: la loro influenza culturale.

3. Una volta discussi con un lobbista di Google i regolamenti sulla divulgazione delle informazioni per etichettare più chiaramente i risultati delle ricerche a pagamento. Il mio interlocutore sembrava non prendere in considerazione l'ipotesi che la legge americana, che prevede una divulgazione trasparente dei finanziamenti, potesse essere applicata sul serio, insistendo che questo tipo di decisioni spetta a Google e solo a Google. Per persone come lui la regolamentazione sarà sempre troppo lenta, maldestra e inefficace. Le mie conversazioni con il personale politico o con membri di alto livello dello staff delle agenzie coinvolte mi hanno dato la sensazione che anche loro abbiano interiorizzato quest'idea.

Tale posizione può incontrare il favore di coloro che, in generale, sono ostili a un eccessivo intervento del governo nell'economia. Tuttavia, molti nelle grandi aziende del comparto tecnologico coltivano una sorta di religione dell'«interferenza» che riecheggia sinistramente il credo della velocità tipico dei futuristi di inizio XX secolo. Esiste una convinzione comune per la quale *tutte* le istituzioni, le culture e le tradizioni umane sono fatte per essere rimpiazzate, o forse migliorate, fino a che cesseranno di esistere. L'apprendimento automatico e l'Intelligenza artificiale (Ai)

vengono visti come «algoritmi dominanti» che prima riprodurranno, poi trascenderanno, infine sostituiranno il pensiero umano.

Un esperto di robotica della Columbia University ha risposto «sarebbe come spiegare Shakespeare a un cane» a chi gli chiedeva di analizzare le richieste rivolte agli scienziati informatici di rendere più trasparenti per gli esseri umani i loro sistemi di Ai. Potrebbe avere ragione fino a quando si tratta di prevedere le condizioni meteorologiche o persino di uccidere le cellule tumorali: in questi casi, effettivamente, non abbiamo bisogno di conoscere il meccanismo di funzionamento esatto di uno strumento di Ai per metterlo nelle condizioni di risolvere i nostri problemi. Ma questi metodi inesplicabili diventano inappropriati quando la posta in gioco sono decisioni importanti che riguardano le persone – per esempio: chi viene assunto, chi licenziato, a chi viene data fiducia o chi viene sanzionato⁵. Un'analoga richiesta di trasparenza e responsabilità dovrebbe valere anche per la programmazione e gli algoritmi che dominano la nostra cultura e la nostra sfera pubblica.

La posta in gioco è alta. L'ordinamento dei risultati da parte dell'algoritmo di YouTube, per esempio, ha scioccato i rappresentanti dei diritti dei minori. La stampa ha scritto che «i bambini sono rimasti traumatizzati dopo aver guardato su applicazioni rivolte a loro video di YouTube che mostravano Peppa Pig con coltelli e pistole». Come ha osservato James Bridle, questo è un problema va ben al di là del semplice decoro: «Quello che più mi preoccupa dei video su Peppa Pig è come queste parodie esplicite e persino le riproduzioni più equivocate interagiscano con le schiere di generatori automatici di contenuti fino a che diventa assolutamente impossibile capire cosa stia succedendo»⁶. Bridle, inoltre, nota altre caratteristiche allarmanti della fiorente industria della generazione automatica di contenuti su YouTube: «La prima è il livello di orrore e violenza che viene messo in onda. A volte è roba che fa inorridire, più spesso sembra trattarsi di qualcosa di molto più profondo e inconscio. (...) La seconda», prosegue Bridle, «è il livello di sfruttamento dei bambini, non in quanto bambini ma perché privi di difese. Sistemi che generano le ricompense in modo automatico come gli algoritmi di YouTube richiedono questo sfruttamento. Stiamo parlando di bambini che, dalla nascita, vengono deliberatamente presi di mira con contenuti che li traumatizzano e li turbano per mezzo di reti che sono particolarmente vulnerabili a questa forma di abuso»⁷.

Un'emittente televisiva ordinaria che mettesse in onda questo sudiciume ne pagherebbe conseguenze che assumerebbero la forma di un calo negli ascolti o di un boicottaggio da parte degli sponsor. YouTube, invece, può definirsi una semplice piattaforma e accusare una moltitudine di creatori di contenuti, programmatori e specialisti dell'ottimizzazione dei motori di ricerca per qualsiasi cosa non vada nel verso giusto⁸.

5. F. PASQUALE, «Reforming the Law of Reputation», *Loyola University Chicago Law Journal*, 47/2015, pp. 515-539, goo.gl/2ddc76

6. J. BRIDLE, «Something is Wrong on the Internet», *Medium*, 6/11/2017, goo.gl/xocED6

7. *Ibidem*.

8. Sul tema si veda F. PASQUALE, «A Silicon Valley Catechism», *Issues in Science and Technology*, vol. XXXIV, n. 1, autunno 2017, goo.gl/5evGnT

4. Autori di contenuti e artisti hanno analizzato i possibili effetti di questa manipolazione comportamentista degli individui da parte di aziende prive di una solida tradizione in materia di rettitudine o buona condotta⁹. Ho definito questo fenomeno «l'individualità dell'algoritmo», perché la coscienza di noi stessi viene codificata in molteplici punti di rilevamento anziché essere incardinata in una tradizione spirituale o in un'identità civica più ampia¹⁰. Nel momento in cui veniamo processati dai computer come un mero flusso di dati, buona parte della nostra umanità va perduta o viene soppressa¹¹.

Non possiamo sperare che sia un'azienda come Facebook a creare una nuova sfera pubblica. I suoi capi confondono il cameratismo superficiale di videogiochi a schermo condiviso per una comunità autentica. L'amministratore delegato di Facebook, Mark Zuckerberg, ha accumulato ricchezza e influenza cercando di monopolizzare il mercato delle interazioni sociali quotidiane anziché provando a risolvere problemi veramente complessi relativi alla produzione di beni reali e servizi. Persino nei settori chiave della sua presunta competenza settoriale, Facebook ha fatto dei compromessi socialmente inaccettabili. In un eloquente profilo di Mark Zuckerberg, Evan Osnos ha notato che «tra la dimensione e la sicurezza, ha scelto la dimensione»¹². Bambini, dissidenti, moderatori di contenuti, proprietari di account hackerati e altre vittime pagano quotidianamente le conseguenze di questa decisione, dal momento che devono sopportare i prevedibili effetti collaterali del gigantismo dei social network.

Analogamente, non possiamo aspettarci che un'azienda come Google si distingua nel preservare le fonti umane di senso e valore. I suoi vertici si sono avvalsi per lungo tempo di Ray Kurzweil, un futurista con una visione decisamente transumanista della natura e del fine del genere umano. Secondo Kurzweil, il nostro destino è quello di fondersi alle, e in ultima istanza essere rimpiazzati dalle macchine¹³. Abbiamo assistito a una piccola sfaccettatura di quest'ambizione nella recente dimostrazione dell'«Assistente Google», una voce dal suono umano che ha il potenziale di ingannare addetti alla reception e persone che fanno lavori simili inducendoli a pensare che chi sta cercando di prendere un appuntamento sia una persona in carne e ossa. Sembra che anche dietro alla funzione «Smart Reply» di Gmail, che riproduce risposte preconfezionate alle e-mail, ci sia la squadra di

9. B. FRISCHMANN, E. SELINGER, *Re-engineering Humanity*, Cambridge 2018, Cambridge University Press; C.S. LEWIS, *The Abolition of Man*, Oxford 1943, Oxford University Press; M.T. ANDERSON, *Feed*, Somerville 2002, Candlewick Press.

10. F. PASQUALE, «The Algorithmic Self», *The Hedgehog Review*, vol. 17, n. 1, primavera 2015, goo.gl/PzBgPH

11. J. SADOWSKI, F. PASQUALE, «The Spectrum of Control», *First Monday*, vol. 20, n. 7, 6/7/2015, goo.gl/Nu5YnT

12. E. OSNOS, «Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?», *The New Yorker*, 17/9/2018, goo.gl/3kTzSJ

13. R. KURZWEIL, *The Age of Spiritual Machines*, New York 1999, Viking Press: «La singolarità tecnologica ci permetterà di superare le limitazioni dei nostri corpi e cervelli biologici. Saremo artefici del nostro destino. La mortalità sarà nelle nostre mani. Saremo capaci di vivere quanto vogliamo». Sul pensiero di Kurzweil si veda C.T. RUBIN, *Eclipse of Man: Human Extinction and the Meaning of Progress*, New York 2014, Encounter Books; R. JONES, *Against Transhumanism*, 2016 (e-book), Soft Machines.

Kurzweil. La funzione, tuttavia, si impappina quando si tratta di comporre pensieri più complessi¹⁴. Il fine ultimo di questa visione del mondo, nonché il fondamento teologico dell'Ai, è la sostituzione degli esseri umani, non fornire loro sostegno.

5. Per Kurzweil e altri futuristi, ha osservato Anthony Galluzzo, «la perfezione umana richiede il superamento del fattore umano»¹⁵. In proposito, Galluzzo cita lo stesso Kurzweil: «La singolarità tecnologica rappresenterà il culmine della fusione del nostro pensiero e della nostra esistenza biologica con la tecnologia di cui disponiamo. Il risultato sarà un mondo ancora umano ma che trascende le nostre radici biologiche. Non ci sarà più alcuna distinzione tra l'umano e la macchina o tra la realtà fisica e quella virtuale. Ciò che rimarrà inequivocabilmente umano in questo mondo è il fatto che la specie umana è l'unica che cerca in maniera innata di estendere le sue possibilità fisiche e mentali oltre le limitazioni correnti»¹⁶. Chi ha una visione più solida e stabile dell'essere umano non se la passerà per niente bene in questo futuro. Non riuscirà a stare al passo di questo delirio tecnologico. Come ha avvertito Francis Fukuyama, l'assenza di una visione condivisa dell'identità umana può essere molto pericolosa per la democrazia.

Quali che siano i guadagni in termini di efficienza apportati dalle grandi aziende del settore tecnologico, queste ultime hanno troppo potere e gli deve essere impedito di fare rilevanti acquisizioni orizzontali. I governi devono smettere di favorirle e il loro status culturale deve cambiare. Le famiglie e le scuole devono mettere in discussione la loro influenza sui bambini. I loro sistemi sono più post-umani che pro-umani, conseguenza naturale del loro impegno a favore di un'«interferenza» che eclissi forme più basilari di attaccamento alle comunità e le fonti istituzionali di senso e valore. Gli approcci algoritmici non sono sempre, e neanche spesso, il modo migliore per comprendere e influenzare il mondo. Non dovremmo permettere che una coalizione illegittima di capi d'azienda e funzionari governativi ce li imponga.

(traduzione di Daniele Santoro)

14. T. SIMONITE, «What is Ray Kurzweil Up to at Google?», *Wired*, 8/2/2017, goo.gl/x4LSC7

15. A. GALLUZZO, «The Singularity in the 1790s: Toward a Prehistory of the Present with William Godwin and Thomas Malthus», *b2o*, 17/9/2018, goo.gl/ovtQbr


16. R. KURZWEIL, *The Age of Spiritual Machines*, cit. in A. Galluzzo, *op. cit.*

PER UNA GEOPOLITICA UMANA APPLICATA AI DATI

di Dario FABBRI

Le potenze, Stati Uniti in testa, accumulano dati che non sanno usare strategicamente. È fuorviante concentrarsi sulla dimensione economica, sulla politica effimera, sui singoli individui. Per capire il mondo conviene studiare le comunità, la loro antropologia.

*Molti dati sono una truffa,
perché molti dati sono stupidi.*
Peter Thiel

1.  DATI INFORMATICI SONO IL SIMBOLO DELLA supremazia americana sul pianeta, insistente ossessione per le potenze che respingono lo status quo internazionale. Ogni giorno miliardi di utenti connessi nel mondo affidano alle aziende high-tech statunitensi innumerevoli messaggi mail, chat, blog, consegnandoli alla disponibilità delle agenzie di intelligence d'Oltreoceano. Mole immensa di informazioni, conservata con l'intento di intuire le tendenze politiche, le preferenze economiche, le evoluzioni sociali, i cambiamenti di umore di individui sparsi sul planisfero, accomunati dall'ingenuità con cui raccontano di sé a un processore. Nelle parole di Tim Berners-Lee, inventore del World Wide Web, «i dati sono la cosa più importante che abbiamo, per questo dureranno più dei sistemi su cui viaggiano»¹.

Tesoro inestimabile per l'analisi economica e politologica. Ma che diventerà strategicamente decisivo soltanto se condotto oltre il contingente, se elevato oltre lo spionaggio. Ovvero se studiato attraverso le categorie della geopolitica umana, approccio capace di liberare le informazioni dalla gabbia tecno-ideologica, di cogliere il destino del pianeta. Indispensabile per stabilire la traiettoria di una potenza, per comprenderne la predisposizione alla violenza, l'attitudine all'egemonia, il collocamento nella storia, per scoprire il rapporto che intrattiene con i ceppi allogeni che ha nel ventre. Eppure poco frequentata dai governi – Stati Uniti compresi – che si battono per i dati senza saperli utilizzare. Tuttora concentrati sulla dimensione economica ed elettorale, impegnati a osservare e prevenire eventi di rilevanza secondaria. Con il rischio di sprecare un immenso patrimonio di nozioni, fornito dagli algoritmi. Per poca frequentazione del fattore umano.

1. Cfr. T. BERNERS-LEE, W. HALL, J. HENDLER, *A Framework for Web Science*, Hanover 2006, Now Publishers.

2. Da sempre lo spionaggio è attività essenziale di ogni potenza. Sapere cosa pensano, cosa progettano antagonisti e alleati è esercizio insostituibile nel perseguimento dell'interesse nazionale. Fin dall'alba dei tempi i governi si sono adoperati per spiare anzitutto i loro cittadini, quindi le personalità più influenti delle comunità vicine. Specie i decisori politici, gli alti ufficiali delle Forze armate, gli scienziati più capaci. Con costi e rischi straordinari per chi era incaricato del compito. Prima che l'avvento di Internet rivoluzionasse tanto fondamentale esercizio.

Scoprire le intenzioni di capi di Stato e militari stranieri resta tra le priorità di ogni intelligence. Ma la diffusione su larga scala di social network, posta elettronica e blog istantanei ha trasferito l'attenzione sulle masse e abbattuto i costi del mestiere. Improvvisamente gli abitanti del pianeta hanno cominciato a comunicare spontaneamente i loro pensieri, perfino i più reconditi, alle multinazionali del Web. Ossia a quelle americane, giacché le omologhe cinesi e russe sono attive esclusivamente sul loro territorio nazionale.

Come dimostrato dal programma Prism, a fronte di nessun pericolo concreto se non in termini di uno scadimento di soft power, da almeno dieci anni la National Security Agency, il ministero statunitense deputato allo spionaggio delle comunicazioni, pesca nei server dei giganti high-tech i dati dell'80% della popolazione mondiale. Segnalati agli analisti dai cosiddetti metadati, funzioni nascoste nell'ipertesto che associano a ogni individuo un particolare pensiero o gesto. Non solo gusti personali e opinioni sul creato. Nei cavi della Rete finiscono atteggiamenti e sentimenti relativi a una comunità, al suo apparente stato di salute o di decadimento.

Di qui un'ossessione minimalista per qualsiasi elemento che riguardi l'economia di una nazione, che disponga di dimensione politica. Tra questi: il livello di benessere reale, al di là di quello misurato dagli indici ufficiali; le simpatie per i partiti convenzionali; la presa di ideologie innovative o conservatrici; il sostegno per gruppi in formazione o in dissoluzione; la rabbia nei confronti della classe dirigente; la superbia e la noia delle élite; la richiesta di cambiamento dell'assetto istituzionale; l'ambizione di una specifica fazione di sostituirsi all'establishment locale; l'adesione a progetti eversivi; la delusione per speranze malriposte; l'influenza o il rigetto provocato sulla popolazione da narrazioni straniere; il tasso di criminalità presente nella società; il rispetto dei diritti umani; le tentazioni autocratiche o terroristiche di cellule sparse.

In nuce, la spasmodica ricerca di strumenti utili per cogliere l'andamento congiunturale di un soggetto statale o informale. Cui si aggiungono i paralleli tentativi di influenzare le dinamiche osservate, di modificare la realtà che poi si riconoscerà nei dati drenati. Attraverso operazioni che oscillano tra il lobbying artificiale e l'offensiva psicologica, in una similguerra (*like war*) di americana definizione². Per cui nei laboratori delle principali potenze nascono notizie false (*fake news*) e troll deputati a smentire esponenti politici e credenze comuni, a sostituire le idee diffuse con opinioni artificiali. Così si fabbricano identità, fatti, report funzionali all'attuale

alternativo degli autori, creati per assurgere a verità quando migliaia di utenti ne abbracciano l'esistenza.

Nuovo corso nella condotta di intelligence, in grado di trasferire la speculazione spionistica dal vertice alla popolazione, dal governante al cittadino, con notevoli benefici per la professione. Ma quasi inutile se mantenuta nell'alveo economico-politologico, se non sostituita con un impianto epistemologico compiuto. Perché fondata sull'illusione che sapere in anticipo per chi voterà una specifica popolazione, di fatto il mestiere di un sondaggista, oppure quanto tempo impiegherà la crisi economica per riverberarsi su una comunità, di fatto il compito di uno statistico, servirebbe a descrivere la parabola del pianeta, sarebbe utile per prevedere cosa si staglia oltre l'immediato orizzonte temporale. Mentre, al di là delle suggestioni, l'adozione di una particolare legge, o anche l'attuazione di un'innovativa politica fiscale, non determinano lo sguardo sul mondo di una collettività, l'approccio nei confronti dei vicini, l'inclinazione dei suoi membri a morire per il bene generale.

Sicché lo scandagliamento dei dati si fa effimero, diviene velleitario intervento sulla loro fruizione, che finisce per magnificare fenomeni spesso ininfluenti sull'andamento della storia, per esaltare questioni che raramente incidono sulla tattica dei soggetti geopolitici, proprio mai sulla loro strategia. Senza comprendere, come spiegato da Albert Einstein, che «non tutto ciò che conta può essere misurato e non tutto ciò che può essere misurato conta».

Intuire la sostituzione – in atto o prossima – di una classe dirigente non preannuncia alcuna svolta concreta, se l'evento non è accompagnato da un cambiamento nelle aspirazioni della popolazione, da un mutamento della sua consistenza etnica, numerica, culturale (oltre che del contesto esterno in cui esiste). Piuttosto, in assenza di tali sviluppi, il futuro establishment è destinato a rincorrere i medesimi obiettivi dei precedenti, pur adoperando una narrazione diversa.

Come capita all'Italia attuale, appena sottoposta a un cambio di dirigenza ma rimasta perfettamente coerente con quanto realizzato negli ultimi anni, nonostante la retorica inedita e gli sforzi profusi da Washington già un decennio fa per conoscere in anteprima i nuovi arrivati³. Quando proprio sul Web cominciò l'interesse dell'amministrazione statunitense per l'allora nascente Movimento 5 Stelle.

Perfino prevedere (o innescare) un cambio di regime non muta per default l'incedere di una potenza, se non si alterano le caratteristiche antropologiche di una popolazione.

La Russia ha attraversato molteplici cambi di costituzione e il saltuario rinnovamento della sua organizzazione statale – dallo zarismo al comunismo, fino all'attuale nazionalismo pseudoreligioso – senza rinunciare alle aspirazioni imperiali, dunque inevitabilmente contraria a chiunque negli anni ne ha benedetto le numerose rivoluzioni. Oppure l'Iraq, inventato dagli americani nella contemporanea configurazione post-Saddam, non aderisce in nulla alle esigenze geopolitiche

3. Cfr. D. FABBRI, «Da Palazzo Chigi a Palazzo Margherita: Leading from Inside?», *Limes*, «L'Italia di nessuno», n. 4/2013, pp. 53-59.

di Washington. Liberato dal giogo baatista, si è rivelato portatore di percezioni e costumi assai vicini all'impero iraniano.

Ancora, indovinare in anticipo la nuova costituzione di uno Stato, non ne stravolge l'esistenza se il sentire dei cittadini si mantiene costante. Una nazione può improvvisamente definirsi repubblica ma nei fatti confermarsi impero, se la sua essenza e i suoi costumi non differiscono dal passato. Oppure viceversa. La Turchia o gli Stati Uniti sono imperi indipendentemente dalla loro dizione istituzionale, mentre il Giappone resta uno Stato nazionale sebbene presieduto da un imperatore.

In tale immutato contesto pure le cosiddette *fake news* non riescono a incidere sui processi strategici. Mentre si trasformano in alibi per candidati sconfitti alle elezioni, pronti ad attribuire a improbabili forze maligne la loro disfatta. Oppure in una giustificazione offerta a governi di ogni tipo per ridurre la libertà d'espressione nei loro paesi, per imporre la propria ortodossa versione dei fatti. Nel pregiudizio, più o meno doloso, che sia necessario difendere i cittadini da sé stessi.

Perché per stabilire i destini del pianeta non basta il minimalismo operativo, è necessario aumentare la profondità dell'indagine. Non è vero quanto sostenuto dal premio Nobel per l'economia, Ronald Coase, per cui «se torturati i dati confessano tutto ciò che sanno»⁴. Serve uno scatto ulteriore. Per individuare gli eventi che altereranno lo status quo internazionale, che sconvolgeranno la gerarchia delle grandi potenze è indispensabile calarsi nella dimensione umana della geopolitica, nelle sue pieghe ineludibili. Specie al contatto con l'elemento cibernetico.

3. Storicamente la geopolitica oscilla tra il determinismo geografico e il volontarismo positivista. Da tempo il suo filone maggioritario sostiene la cogente relazione tra il territorio e il destino dei popoli, descrivendo la matrice fisico-climatica come artefice della vicenda umana. Nella massima del geografo inglese Halford Mackinder: «L'uomo può agire, ma la natura in larga parte lo controlla»⁵. Visione forzata, ancorché affascinante, ripresa negli ultimi anni da acuti neodeterministi come Robert Kaplan⁶, che svela monca una disciplina che si vorrebbe universale. Fino a scadere in un plateale razzismo, intriso di etnografia.

A tale concezione si oppone il tentativo soprattutto del possibilismo francese di tradurre gli inderogabili limiti della geografia in direzione arbitraria. Specie nel lavoro di Paul Vidal de la Blache⁷ e dei suoi adepti, disposti a riconoscere alle nazioni e agli imperi un notevole ethos di possibilità. Nobile sforzo, pensato per conciliare il libero arbitrio kantiano con l'estremismo geografico – oltre che la Francia di fine Ottocento con la sconfitta subita dalla Prussia. Di recente (parzialmente) recuperato da geografi critici come John Agnew e Simon Dalby, per i quali sarebbe necessario un possibilismo che esalti il legame tra la fisicità della terra e l'ecologia

4. Massima pronunciata da Coase in una lezione all'Università della Virginia nel 1962.

5. Cfr. H. MACKINDER, *Democratic ideals and reality*, London 1942, Constables.

6. Cfr. R. KAPLAN, *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*, New York City 2012, Random House.

7. Cfr. V. BERDOULAY, *La formation de l'école française de géographie (1870-1914)*, Paris 1981, Le Comité des travaux historiques et scientifiques (Cths).

politica. Se non fosse che l'iniziativa finisce per giustificare l'umano desiderio di imporsi irrealisticamente sulla condizione terrestre. Fino a riconoscere drammatico rilievo alla politologia, disciplina tendente all'innamoramento per categorie improbabili, incapace di cogliere il rapporto di causalità tra i fatti.

Mentre per conferire equilibrio alla geopolitica, per allontanarla contemporaneamente dalle secche del determinismo e del volontarismo, è necessario astrarsi dall'individuo per concentrarsi sulle collettività, sintesi palese tra le imposizioni dell'ambiente e le creazioni dell'uomo. Adottare una geopolitica umana che riconosca a Stati e imperi caratteristiche estranee alla sola origine geografica, senza precipitare nel velleitario autismo della politica.

Così per rendere efficace lo studio dei dati, per superare il semplice computo numerico, è indispensabile abbandonare l'analisi dei singoli individui, per considerarli espressione di una specifica comunità, in grado di esistere nella storia soltanto in forma aggregata, attraverso un sentire spesso inconsapevole. Applicando agli algoritmi specifici filtri antropologici, gli unici che segnalano inclinazioni consistenti della traiettoria strategica. Dagli effetti demografici al collocamento storico di una nazione, dall'atteggiamento nei confronti dell'immigrazione al costume generale, dall'individuazione di una missione condivisa al riconoscimento di capacità diffuse.

Anzitutto, la demografia. Stabilire il nesso esistente tra l'età mediana di una nazione e il suo sguardo sul mondo è esercizio potenzialmente decisivo per descrivere il futuro, al di là della predisposizione a riprodursi. Una potenza anagraficamente giovane si mostra propensa, nella fase attuale oppure nel medio periodo, a imporsi con violenza sul contesto internazionale, a credere che i massimi sistemi siano nella sua disponibilità, a sopportare i sacrifici di un'impresa gravosa, a commettere plateali ingiustizie per sopravvivere. Se necessario a fare la guerra per ottenere ciò che desidera, sfidando egemoni regionali o globali. Specie se dispone di tradizione bellicosa e spiccate conoscenze tecnologiche.

Dunque cogliere in una popolazione, attraverso i dati, il mantenimento di un atteggiamento edonistico o frugale, oppure l'esaltazione dell'individualismo o la sua condanna, può risultare molto più rilevante che studiare le intenzioni di voto. Nozioni facilmente rintracciabili nelle opinioni consegnate al Web, se scrutate con occhio consapevole. In post che palesano un atteggiamento di ammirazione o di scherno nei confronti delle famiglie numerose, che esaltano un esuberante militarismo o condannano ogni unilateralismo, che accettano seraficamente l'esistenza delle ingiustizie sociali o che vorrebbero risolverle tutte.

Tali evidenze potrebbero collocare una collettività tra le potenze correnti o passate, tra la storia e la post-storia. In caso di dimensione storica, potrebbero elevare il soggetto a potenziale antagonista dell'egemone planetario, pure se formalmente alleato. È il caso della Turchia vista nel lungo periodo, oppure della Francia. Stati segnati da un notevole cambiamento demografico e massicciamente aperti ai social network di origine statunitense. Destinati ad aumentare il loro peso nel mondo, a patto di assimilare i gruppi alloigeni presenti sul territorio. Specie l'E-

sagono, tuttora stretto tra integrazione e assimilazione, altri elementi indispensabili della geopolitica umana.

Indagare come un soggetto si relaziona con i ceppi allogeni presenti sul suo territorio fornisce informazioni preziose sul momento cronologico vissuto dalla sua popolazione, sul grado di indipendenza di cui dispone, su ciò che vorrà essere in futuro. Integrare gli immigrati significa indurli ad accettare il codice civile della società adottiva, renderli partecipi della comunità, pur conservandone l'alterità. Assimilare, invece, comporta l'introduzione degli stranieri nel tessuto antropologico della popolazione, renderli indistinguibili dagli altri cittadini. Senza consentire loro di mantenere alcuna specificità, se non quella del paese d'approdo.

Processi che richiedono risoluzioni diverse, con l'assimilazione che prevede l'impiego di una notevole dose di violenza e conseguente limitazione delle libertà personali, anche ai danni del ceppo originario. Per questo soltanto una popolazione mediamente giovane e feroce può sostenerne la crudezza, perché intenzionata a rendere omogenea la popolazione in vista di una prossima guerra, perché pronta ad affrancarsi dalla sfera di influenza cui appartiene, se non già libera da tanta costrizione. Non a caso solamente gli Stati Uniti e i loro principali antagonisti sono in grado di realizzare l'assimilazione. Mentre qualsiasi altra nazione che ne volesse emulare il proposito finirebbe nel mirino dell'egemone. Come recentemente capitato alla Cina, con le accuse avanzate da Washington per il presunto tentativo di assimilare forzatamente gli uiguri.

Le informazioni cibernetiche potrebbero fornire cruciali segnali in merito. Qualora registrassero un atteggiamento al contempo di apertura e di violenza nei confronti degli immigrati, piuttosto che l'intenzione di condurre dolorosamente al conformismo i nuovi arrivati anziché espellerli dal territorio, oppure se carpissero una narrazione universalistica della locale etnicità, che la renda abbracciabile da chiunque.

Ancora, la geopolitica umana offre all'intelligence gli strumenti per discernere di cosa vive uno specifico popolo, se di soddisfazioni personali o collettive, se di economia o di status strategico. Se in una nazione è moneta sonante soltanto il denaro o anche la gloria, l'affermazione dei singoli cittadini o della nazione.

Discrimine sufficiente a descrivere gli obiettivi ancestrali di uno specifico soggetto, la sua capacità di esistere al di là della taglia economica, di sopportare le avversità finanziarie, endogene o indotte. Quanto facilmente verificabile con lo studio di mail e affini perché riguardante il momento attuale. Fondamentale segnale della possibilità per una nazione di soccombere o di resistere in caso di sanzioni economiche o di umiliazione internazionale della sua classe dirigente. Per cui esistono paesi storicamente indigenti, come Russia, Iran o Vietnam, che si mostrano disposti a sostituire la mancata ricchezza materiale con il proprio status strategico. E altre nazioni, come quelle dell'Europa occidentale, incapaci di sopportare sacrifici di lungo termine per moltiplicare la propria rilevanza, per conservare un orgoglio collettivo.

Infine, tra quanto fornito dai dati andrebbe ricercato il livello di disciplina sociale che contraddistingue una comunità. Disposizione essenziale per centrare traguardi faticosi, per non sfiarsi prima di raggiungere il risultato anelato, per assorbire perdite e sconfitte, per imporre il sacrificio maggiore di un'avventura a una sola parte della collettività. Strumento utilizzato dalle grandi potenze per reagire alle circostanze avverse, per supplire a una deprimente demografia o a un evidente gap tecnologico. Dimenticato nell'analisi dei dati, quasi fosse meno importante dell'ascesa o del declino di una particolare ideologia. Eppure facilmente intuibile nelle comunicazioni e nei post degli utenti, non appena questi dichiarano la loro sentita appartenenza alla causa nazionale, indipendentemente dall'estrazione politica della classe dirigente, non appena denotano normalità nell'accollarsi il debito di una parte del paese. Come capita al Giappone⁸ o alla Russia, declinanti sul piano demografico ma parossistici nella difesa delle loro convinzioni.

Grandezze insostituibili per comprendere le dinamiche internazionali, per prevedere cosa accadrà al pianeta. Ma osservabili soltanto con i mezzi della geopolitica umana, il migliore sistema di navigazione tra miliardi di dati. Pressoché sconosciuto a intelligence e classe politica.

4. Confitto in una condizione imperfetta e dolorosa, l'uomo si innamora puntualmente della tecnologia, confidando nella scienza per trascendere la propria natura. Alle prese con i dati si fissa sulla quantità, sui parametri, sulla corrispondenza tra costi e azione. Finisce per concentrarsi su aspetti minori della propria esistenza. Esalta i dettagli, scambiandoli per massimi sistemi, abbraccia i contorni, ponendoli al centro della sua speculazione. Quasi vivesse soltanto di individualità. Quasi fosse guidato da mere considerazioni utilitaristiche.

Tanto miope minimalismo intrappola analisti e osservatori in questioni superficiali, preclude la visione di insieme. Mentre ciò che determina il destino del globo si dipana sulle loro teste. È di matrice qualitativa, prescinde dagli algoritmi, incrocia percezioni e sentimenti diffusi. Spesso manca di logicità, si nutre di massimalismo, antepone l'azione alla felicità, si disinteressa del giusto per perseguire l'emozionale. Soprattutto riguarda le collettività, l'inconscia adesione degli individui a una nazione. Oltre ogni volontà, sono le caratteristiche di una comunità a imporsi sugli eventi. È la diffusa capacità (o incapacità) di un popolo di stare al mondo a determinare la sorte degli individui, è la cittadinanza a condurre gli uomini in guerra, non l'appartenenza religiosa o di classe, è l'età mediana a segnare possibilità e chimere, non le singole anagrafi. Chi vorrà domare la tecnologia, capire che sarà del pianeta, dovrà necessariamente recuperare tale consapevolezza. Andare oltre la matematica, l'economia, la tecnologia. Aumentare la scala d'indagine, passare dal micro al macro. Affidandosi al sentire ancestrale della geopolitica umana. All'unico metadato in grado di collegare le informazioni tra loro, all'unico chip che può rendere intellegibile la complessità del pianeta. Passaggio obbligato tra la realtà e il cibernetic.

8. Cfr. D. FABBRI, «L'importanza di essere Giappone», *Limes*, «La rivoluzione giapponese», n. 2/2018, pp. 33-45.


LE FAKE NEWS SPECCHIO DELL'ANIMA DELLA SILICON VALLEY

di Niccolò LOCATELLI

Lo spettro della disinformazione russa è il pretesto di stampa, Congresso e apparati per tenere sulla graticola i giganti californiani della Rete. Tanto importanti per la proiezione della potenza statunitense quanto restii a sentirsene parte. La Cina, suo malgrado, li salverà.

Senza Facebook non avremmo vinto.
Theresa Hong, responsabile dei contenuti digitali
per la campagna elettorale di Donald Trump

*L'idea che le fake news su Facebook
abbiano influito sulle elezioni è una follia.*
Mark Zuckerberg¹

1.  SECONDO I DIZIONARI, LA «NOTIZIA» È un'informazione che rende noto un fatto; il «fatto» è qualcosa che è accaduto; «falso» è qualcosa di non vero, che non corrisponde nella realtà a ciò che sembra essere. Pertanto una *fake news*, in italiano «notizia falsa», è nel più poetico dei casi un ossimoro e nel più prosaico una contraddizione in termini. Qualcosa che non esiste o che ha bisogno di una definizione corretta, appurato che «disinformazione» dev'essere un lemma poco smart per il XXI secolo, probabilmente perché non deriva dall'inglese.

Priva di senso lessicale, l'espressione non è però priva di senso geopolitico. Anzi, il prisma – lo spauracchio – delle *fake news* fornisce un'ulteriore chiave di lettura all'offensiva di Washington contro i suoi due principali avversari geopolitici (Russia e Cina) e rivela l'importanza della Silicon Valley nella proiezione della potenza a stelle e strisce. Alcune circostanze della vittoria di Donald Trump hanno scoperto un vaso di Pandora che le imprese digitali californiane non riusciranno a chiudere, ma sono chiamate a provare almeno a socchiudere.

La questione della disinformazione diventa popolare con l'espressione *fake news* nel dibattito relativo alle elezioni presidenziali dell'8 novembre 2016. Quasi nessuno aveva previsto che un palazzinaro invisibile al suo stesso partito e incline allo scandalo come il repubblicano Donald Trump potesse sconfiggere una profes-

1. Entrambi citati in E. OSNOS, «Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?», *The New Yorker*, 17/9/2018, [is.gd/54RVQx](https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy)

sionista della politica come la candidata democratica Hillary Clinton. A urne chiuse e con il senno di poi sarebbe stato possibile individuare diverse ragioni plausibili della *débâcle* clintoniana, dal rigetto verso una figura percepita come elitaria all'innata abilità trumpiana nel rappresentare le paure dell'America bianca. Nella narrazione post-8 novembre alimentata dall'ex *first lady* e ripresa dai mezzi d'informazione tradizionali hanno invece prevalso altri aspetti: l'operato dell'allora direttore dell'Fbi James Comey² e l'attacco russo alla democrazia statunitense, di cui la disinformazione su Facebook, Twitter, Reddit e altri canali della Rete sarebbe stata una componente rilevante.

L'11 gennaio 2017 l'allora presidente eletto rifiuta di rispondere alle domande del giornalista di Cnn accusando lui e l'emittente per cui lavora di «essere una *fake news*»³. Inserita nella narrazione di Trump, basata sulla delegittimazione del sistema politico-mediatico preesistente e contrario al suo arrivo alla Casa Bianca, l'espressione da quel momento permea il dibattito statunitense e internazionale sulla disinformazione, in particolare quella riconducibile alla Russia.

2. Stando al rapporto rilasciato dal direttore dell'intelligence nazionale Usa il 6 gennaio 2017, Vladimir Putin ha ordito l'attacco più vasto di sempre contro le presidenziali per minare la fiducia mondiale nel processo elettorale statunitense e nell'ordine liberaldemocratico guidato da Washington. L'offensiva ha preso varie forme: dai tentativi falliti di manomettere i sistemi elettronici di voto fino alle intrusioni di pirati informatici nei server del Partito democratico, passando per la collaborazione con WikiLeaks e la denigrazione di Hillary Clinton attraverso canali quali Russia Today, siti come Sputnik, troll «quasi-governativi» sui social media. L'indagine del procuratore speciale Robert Mueller, che copre anche questi temi, ha già portato alle prime condanne. Né il rapporto né la causa di Mueller relativa alla disinformazione utilizzano l'espressione *fake news*⁴.

Che il Cremlino abbia provato a influenzare le elezioni presidenziali statunitensi del 2016 è innegabile e, da un punto di vista geopolitico, ineccepibile. La salute della Russia dipende anche dal miglioramento dei rapporti con la superpotenza. Dopo l'annessione della Crimea, le sanzioni occidentali imposte da Washington – anche agli alleati europei – hanno allontanato Mosca dal Vecchio Continente spingendola verso la Cina, che rimane un rivale strategico per giunta meno avanzato

2. «È stato il fattore più importante nella mia sconfitta», ha detto la candidata democratica nella prima intervista dopo le elezioni. *Hillary Clinton: "I was dumbfounded" by James Comey letter on Oct. 28*, buff.ly/2z18wXc. Il 28 ottobre 2016 James Comey inviò al Senato una lettera – resa pubblica – per annunciare la revisione dei messaggi di posta elettronica trovati sul computer del marito di un'assistente di Clinton. Il 6 novembre, due giorni prima delle elezioni, segnalò con un'altra lettera che dalla revisione delle mail non era emerso nulla di rilevante ai fini dell'indagine. Sull'importanza della sua decisione, cfr. N. SILVER, *The Comey Letter Probably Cost Clinton The Election*, buff.ly/2qQbMzt. Per ironia della sorte, Comey – licenziato da Trump nel maggio 2017 – ha svolto parte del suo lavoro di direttore dell'Fbi usando un account personale di posta Gmail.

3. «Non accetto domande da te, il tuo canale... tu fai *fake news*». Donald Trump al giornalista di Cnn Jim Acosta durante la conferenza stampa da presidente eletto, 11/1/2017.

4. *Assessing Russian Activities and Intentions in Recent US Elections*, Office of the Director of National Intelligence, 6/1/2017, goo.gl/FAh81z

tecnologicamente degli Usa. Di fronte alla continuità promessa da Hillary Clinton, aveva senso sostenere il candidato meno russofobo, oltre che meno esperto.

Che tra i mezzi per influenzare i processi politici ci sia la disinformazione online non è una novità. Appena un lustro prima delle presidenziali, l'Occidente aveva incensato il ruolo dei social network nelle cosiddette primavere arabe. Facebook e Twitter avevano permesso ai manifestanti di coordinarsi superando la censura di regime sui media tradizionali. Curiosamente, non erano stati stigmatizzati come *fake news* i ripetuti annunci sulla morte di Mubarak e al-Asad (tuttora in vita) o il racconto di stragi che Gheddafi non aveva (ancora) compiuto. Nel 2009, nessuno si era indignato per la richiesta – accolta – del dipartimento di Stato a Twitter di rinviare la chiusura momentanea per manutenzione della piattaforma digitale proprio mentre infuriavano le proteste dell'Onda verde contro la conferma di Ahmadi-Nejad alla presidenza dell'Iran.

La novità dell'operato russo nel 2016 è stata la capacità di raggiungere un numero rilevante di elettori effettivi o potenziali sfruttando strumenti inventati dal suo bersaglio – Internet è pur sempre una creazione delle Forze armate degli Stati Uniti. Mosca ha evidentemente fatto tesoro dell'esperienza accumulata tra il 2012 e il 2014, quando aveva prodotto *dezinformacija* sulle manifestazioni anti-putiniane e sul conflitto in Ucraina⁵.

Secondo l'inchiesta di Mueller, l'attività online russa è stata coordinata dall'Agenzia di ricerca su Internet (Ira). Nota in Occidente come «fabbrica dei troll», l'Ira aveva (ha) a disposizione circa un milione di dollari al mese e centinaia di persone. I suoi troll hanno creato pagine e profili fasulli, molti dei quali automatizzati (bot), usando se necessario i dati rubati a cittadini statunitensi⁶. L'obiettivo tattico era favorire la vittoria di Trump, quello strategico polarizzare la società statunitense, sfruttandone le fratture lungo alcune linee di faglia – razza, religione, classe, genere, orientamento sessuale – e postando se necessario contenuti di significato opposto nello stesso momento.

Almeno su Facebook, sono stati raggiunti entrambi gli obiettivi: i post più condivisi tra tutti quelli contenenti disinformazione (compresi quelli legati alla Russia) non riguardano né Clinton né Trump, ma Obama, e devono il loro successo alla narrazione per cui il presidente afroamericano forse è musulmano e forse non è americano⁷.

In base ai dati disponibili a ottobre 2018, l'agenzia russa ha gestito la pubblicazione di oltre 9 milioni di tweet tra il 2013 e il 2018, di oltre 80 mila post organici e di 3.519 post sponsorizzati su Facebook tra il 2015 e il 2017. Il social network co-fondato da Mark Zuckerberg ha stimato che 126 milioni di suoi utenti hanno visualizzato dei contenuti *made in Ira* – compresi i cittadini di altri pa-

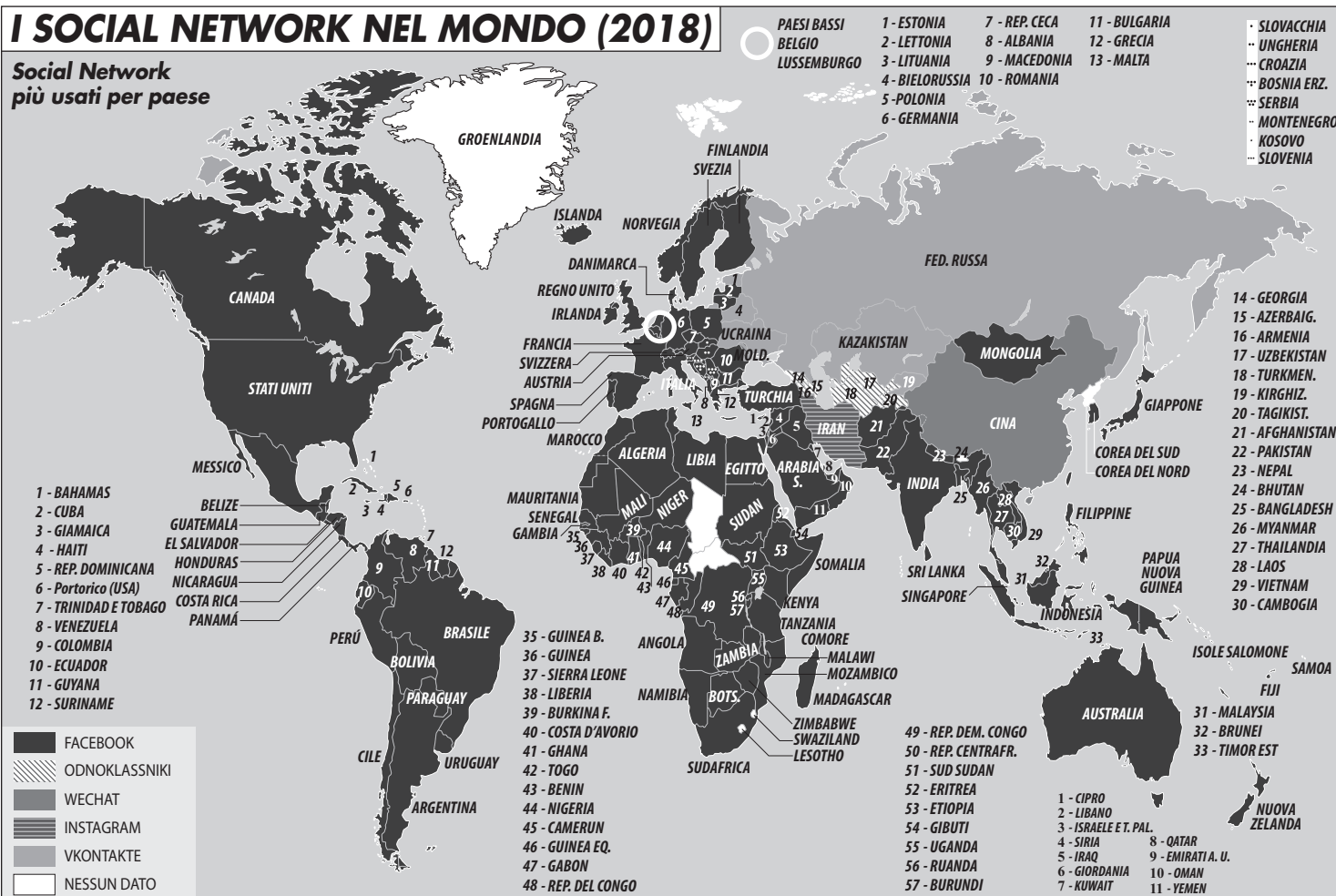
5. #TrollTracker: Twitter Troll Farm Archives, AtlanticCouncil – Digital Forensic Research Lab, goo.gl/QcVG6x. Internet Research Agency Indictment – Department of Justice, 16/2/2018 goo.gl/n1qNqf

6. S. FISHER, «Lessons about Russian Social Media Meddling from Mueller's Indictment», *Axios*, 17/2/2018, buff.ly/2Sil856

7. *Most Popular Fake Election Stories in the United States in 2016, by Facebook engagement (in thousands)*, goo.gl/9i97H8

I SOCIAL NETWORK NEL MONDO (2018)

Social Network
più usati per paese



LE FAKE NEWS, SPECCHIO DELL'ANIMA DELLA SILICON VALLEY

Fonte: Vincenzo Cosenza su dati Alexa e Similar Web.

esi, gli americani privi del diritto di voto e gli stessi bot russi che si seguivano a vicenda.

I numeri paiono impressionanti ma non lo sono. A fronte del milione di dollari abbondante di budget mensile dell'Ira, Trump ne ha spesi 617 per tutta la campagna elettorale, Clinton più di un miliardo. I tweet dei bot russi hanno rappresentato l'1% dei tweet in materia elettorale apparsi sulla piattaforma nei due mesi e mezzo precedenti il voto. Il numero di utenti che ha visualizzato contenuti creati dall'Ira su Facebook è di poco inferiore alla somma dei voti presi l'8 novembre da Clinton e Trump (65.8 + 62.9 milioni). Ma se questi post sono stati visti da quasi tutti i votanti, la loro rilevanza è nulla⁸.

Mosca ha mostrato di conoscere tutte le fratture che vengono solitamente nascoste dal sogno americano. Ma nel soffiarvi sul fuoco, ha rafforzato orientamenti pregressi più che indurre un cambiamento nel voto⁹. Per le *fake news*, come del resto per il *fact checking*, è difficile uscire dalle rispettive camere dell'eco.

Big data alla mano, affermare che la disinformazione elettorale prodotta dai russi sia stata determinante ai fini della sconfitta di Clinton è dunque una grossolana esagerazione. Come è difficile pensare che possa esserlo (stata) in altre elezioni non solo statunitensi, a prescindere dall'origine russa o meno del messaggio. Naturalmente, ciò non ha dissuaso vari attori dal gridare allo scandalo *fake news* per colpire Trump, la Russia e la Silicon Valley.

3. Pentagono, comunità dell'intelligence e dipartimento di Stato – gli apparati – sono favorevoli a delegittimare un presidente anticonvenzionale come Trump, la cui pur volubile agenda personale confligge con gli interessi nazionali in alcuni punti, tra cui il mantenimento della presenza militare nel mondo e dell'ostilità verso Mosca. Vincolare il suo arrivo alla Casa Bianca all'intervento segreto di una potenza straniera che l'opinione pubblica storicamente percepisce come nemica può indebolirlo e limitarne le sortite non previamente concordate su temi internazionali. A questo scopo, il dibattito attorno alle *fake news* e alle responsabilità dei social network è molto più immediato del freddo lessico legalistico che inevitabilmente pervade le indagini di Mueller.

Il Congresso partecipa alla proiezione globale degli Usa e condivide l'impostazione russofoba degli apparati. Ma la sua ostilità a Trump è politica prima che geopolitica: lo scontro classico tra legislativo ed esecutivo è acuito dalla presenza alla Casa Bianca di un corpo estraneo allo stesso partito che l'ha suo malgrado sostenuto.

I mezzi di informazione tradizionali hanno contribuito – loro sì – in maniera decisiva all'ascesa del magnate newyorkese, dandogli ampio spazio prima ancora

8. Sui budget di Ira, Clinton e Trump cfr. N. SILVER, *How Much Did Russian Interference Affect The 2016 Election?*, 16/2/2018, buff.ly/2D59dDi. I dati sui tweet sono tratti da *Twitter, Inc. United States Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism Update on Results of Retrospective Review of Russian-Related Election Activity*, 19/1/2019 (sic), goo.gl/WaWcbW. I dati del voto popolare sono tratti da *Official 2016 Presidential General Election Results*, goo.gl/TXUu6A.

9. A. GUESS, B. NYHAN, J. REIFLER, *Selective Exposure to Misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign*, 9/1/2018, goo.gl/oux26k

che ottenesse la nomina dai repubblicani. Le posizioni controverse, la retorica divisiva, gli stessi attacchi ai media convenzionali lo rendevano l'unica figura in grado di generare interesse (quindi spettatori, copie e spazi pubblicitari venduti) per un'elezione in cui la facile vittoria di Hillary Clinton pareva scontata. I benefici economici di questa strategia perdurano¹⁰, ma il trionfo trumpiano ha messo a nudo la debolezza di stampa, radio e televisioni, rivelatesi incapaci di capire e orientare l'elettorato¹¹ e minacciate dalla comunicazione digitale. L'insistenza sul legame tra la disinformazione online di origine russa e la presenza di Trump alla Casa Bianca è per il Quarto Potere – prima ancora che una battaglia democratica – una questione di affari. Il bersaglio principale non è Mosca e nemmeno il successore di Obama: è la Silicon Valley.

Per i media tradizionali, Internet significa nuovi canali di propagazione delle informazioni, gestiti però tramite algoritmi ignoti e costantemente modificati; nuovi concorrenti, dai blog ai profili Instagram, spesso meno qualificati e sempre con spese di produzione inferiori; infine, minori ricavi dalla pubblicità, visto che i Gafa (Google, Apple, Facebook e Amazon) dominano e dettano le condizioni anche nel settore promozionale.

Suonare l'allarme per le *fake news* permette al Quarto Potere di esporre il problema principale dell'informazione creata online: l'assenza di un controllo che preceda la pubblicazione, mascherato dalla sbandierata neutralità delle piattaforme digitali e dal pronto intervento *ex post* in caso vengano segnalati abusi. Un problema intrinseco al modello di affari basato su rapidità, automazione e grandi numeri – aggravato dalla possibilità di sponsorizzare i propri contenuti per aumentarne in maniera rapida, automatizzata e quantificabile la visibilità.

Anche la diffidenza di apparati e Congresso verso i giganti di Internet basati in California ha origini profonde, che il fenomeno delle *fake news* ha contribuito a portare a galla.

La Silicon Valley pone un problema che Detroit (auto), Houston (idrocarburi), Hollywood (cinema), Wall Street (finanza), naturalmente il Medio Atlantico (difesa) e persino Seattle (Microsoft e Amazon) non pongono. Dalla privacy alla neutralità della Rete, dall'opportunità di lavorare con/per il Pentagono alla presenza sul mercato cinese, la Silicon Valley ha un'agenda – oggetto di un vivace dibattito interno cui per motivi di immagine dà ampia rilevanza – che non è sempre allineata a quella di Washington. Caratteristica difficile da immaginare per gli altri grandi settori industriali del paese. Google, Apple, Facebook, Twitter (da ora in poi, Gafa) non saranno mai intenzionalmente antiamericani e hanno già dato prova della loro disponibilità a collaborare con le istituzioni, ma a differenza di Amazon non sono

10. P. VERNON, «Subscription Surges and Record Audiences Follow Trump's Election», *Columbia Journalism Review*, 6/12/2016, goo.gl/FXZnxo

11. Delle prime 97 testate del paese, 57 si erano schierate con Clinton, 3 contro Trump, 2 con Trump. The American Presidency Project, *2016 General Election Editorial Endorsements by Major Newspapers*, buff.ly/2R5CMHM. Nel suo ultimo aggiornamento prima dello scrutinio, la sera dell'8 novembre, il *New York Times* dava a Hillary Clinton l'85% di probabilità di vincere le elezioni. J. KATZ, «2016 Election Forecast: Who Will Be President?», *The New York Times*, 8/12/2016, buff.ly/2S60Iw0

ancora divenute organiche alla potenza americana. Certo, il settore è giovane, come giovani sono i suoi vertici e recente il loro impegno nel lobbying a Washington¹². E l'humus libertario della Baia di San Francisco nel quale proliferano queste aziende incoraggia una certa resistenza all'autorità. Ma al di là del fattore tempo e del fattore spazio, finora è mancata l'ambizione di integrarsi nel sistema di potere a stelle e strisce. L'intrinseca proiezione internazionale di Internet ha accresciuto il *soft power* degli Usa (basti pensare al dilagare degli anglicismi nelle lingue neolatine) ma ha indotto i Gafa a elaborare da subito una strategia su scala globale, non nazionale. Nel 2018, più della metà dei loro ricavi deriva dai mercati mondiali¹³. Ciò li spinge a favorire una logica di abbattimento delle barriere che ha spalancato le porte alla disinformazione alimentata da potenze straniere nemiche.

Il tema si fa più pressante quanto più cresce il ruolo della tecnologia dell'informazione non solo nel settore della difesa, ma nella vita di ogni cittadino. Internet abbatte costi e tempi; valorizza l'intelligenza artificiale quantitativa più di quella umana qualitativa, che pure l'ha creata; induce l'illusione che il valore di beni e servizi sia nella loro misurabilità e ne altera la fruizione e le aspettative al riguardo anche quando si è offline. L'offerta politica deve rapidamente adeguarsi a un linguaggio nuovo e a un orizzonte temporale accelerato e ristretto da social network e motori di ricerca. Apple News (che è rimasta immune allo scandalo *fake news*) Google News, YouTube, Facebook e Twitter premiano la nicchia rispetto alla totalità, l'immediatezza rispetto all'approfondimento, l'aggiornamento continuo rispetto alla costanza, l'emozione rispetto alla riflessione. «Gli individui diventano dati e i dati comandano», per dirla con un angosciato Henry Kissinger¹⁴.

Il Congresso condivide le preoccupazioni generali verso i giganti della Rete, a partire dalla diffidenza verso un mondo che non conosce e non capisce fino in fondo, e ne aggiunge di specifiche riguardanti la propria sopravvivenza. In un sistema digitale che premia le nicchie, la disinformazione veicolata dai social media può essere più efficace a livello locale che nazionale e il suo impatto su un'elezione legislativa maggiore che su quella presidenziale. A proposito di presidenti: il viaggio intrapreso nella pancia degli Stati Uniti da Zuckerberg subito dopo la vittoria di Trump è stato interpretato come l'annuncio implicito di una sua candidatura. Posto che per il creatore di un'impresa che ha oltre due miliardi di clienti al mese – di cui appena il 10% da Stati Uniti e Canada¹⁵ – persino la Casa Bianca rischia di

12. Internet è appena al 15° posto tra i settori più attivi nel lobbying; tra le prime 10 imprese che spendono di più nel lobbying, dei Gafa c'è solo Alphabet, la società che controlla Google. Dati tratti da www.opensecrets.org

13. Fa eccezione Twitter, che ricava dall'estero «appena» il 46,5% del totale. Dati riferiti al secondo o terzo quadrimestre 2018. Per Alphabet (Google) goo.gl/TVEzwx. Per Apple goo.gl/6TxVZU. Per Facebook goo.gl/xDv9Jv. Per Twitter buff.ly/2SowxjC

14. H.A. KISSINGER, «How the Enlightenment Ends», *The Atlantic*, 15/5/2018, goo.gl/UwaEuG. Il discorso è valido anche per altri due social network di proprietà di Facebook – Instagram e WhatsApp, nuova frontiera della disinformazione – e per Netflix, in grado sinora di evitare le polemiche politiche presentandosi come un'impresa di puro intrattenimento.

15. Gli utenti attivi mensilmente su Facebook tra maggio e agosto 2018 hanno raggiunto i 2 miliardi 234 milioni, record. Di questi, solo 241 risiedono negli Usa o in Canada. *Facebook Q2 2018 Results*, goo.gl/xjcQwq

essere riduttiva, la sua discesa in campo potrebbe rivoluzionare il sistema partitico statunitense. A suggerire il rinvio del suo ingresso in politica sono stati lo stillicidio di notizie relative alle attività di troll russi su Facebook, lo scandalo di Cambridge Analytica e i dubbi sulla neutralità degli algoritmi (e delle persone) di Menlo Park. Zuck, che in epoca obamiana aveva assunto posizioni progressiste sui diritti di lesbiche, gay, bisessuali o transgender e sui migranti, si è ritrovato nel giro di pochi mesi a doversi difendere dall'accusa di aver fatto vincere Trump e da quella di sopprimere sul suo social media le notizie riconducibili a posizioni conservatrici. La sua reazione all'accusa di aver lasciato spazio alle *fake news* è stata ridurre lo spazio a tutte le *news*, modificando l'algoritmo di Facebook in maniera da dar maggiore risalto ai post di carattere personale. Accuse simili hanno colpito Twitter e – con qualche ragione – Google¹⁶.

4. Alimentato da media tradizionali, apparati e Congresso, l'allarme generato dalla disinformazione russa ha cambiato il clima attorno ai social network, avviando un calo della fiducia nei loro confronti che si è accentuato (in particolare per Facebook) con lo scandalo di Cambridge Analytica e con le successive violazioni dei dati¹⁷. I motori di ricerca, i social media e i loro fondatori sono sulla graticola e nessuno ha interesse a toglierli da lì.

Gli interessi nazionali sconsigliano però al Congresso di prendere due misure che risolverebbero la questione delle *fake news* ma segnerebbero la fine dei Gaft per come li abbiamo conosciuti sinora. La prima sarebbe la loro sostanziale equiparazione alle imprese editoriali, con obbligo di un controllo preventivo sui contenuti pubblicati e responsabilità legali sugli stessi. Per essere efficace, tale controllo preventivo dovrebbe essere qualitativo e quindi operato da molti esseri umani in un lasso di tempo inevitabilmente non breve. Divenendo così inconciliabile con il modello di affari basato su rapidità, automazione e un paniere immenso di utenti (con relativi dati) adottato dai giganti della Rete, che non a caso insistono a definirsi imprese tecnologiche, non editoriali. Le concessioni di Google, Facebook, Twitter ed Apple News in occasione delle elezioni di metà mandato statunitensi sono simboliche ed estemporanee, non strutturali: lo stesso Zuckerberg ha riconosciuto al Congresso che l'unica soluzione attuabile su grande scala è il ricorso all'intelligenza artificiale, malgrado gli evidenti limiti dell'approccio quantitativo siano stati confermati proprio dai rimedi cercati dai Gaft¹⁸.

16. Prima è emerso un video in cui i vertici dell'azienda controllata da Alphabet si lamentavano dell'esito delle presidenziali, poi un carteggio telematico in cui alcuni lavoratori proponevano di alterare i risultati di ricerca per contrastare gli ordini esecutivi che negano l'ingresso ai cittadini provenienti da alcuni paesi a maggioranza islamica (il cosiddetto *Travel ban*). Google sostiene che la proposta non sia stata accolta.

17. *Digital News Reports 2018*, www.digitalnewsreport.org

18. D. HARWELL, «AI Will Solve Facebook's Most Vexing Problems, Mark Zuckerberg Says. Just Don't Ask When or How», *The Washington Post*, 11/4/2018, wapo.st/2qn5qJj. La *war room* allestita da Facebook per combattere in tempo reale la disinformazione in occasione delle elezioni brasiliane e di quelle statunitensi di metà mandato constava di una ventina di persone. R. JONES, «Facebook's War Room Is Definitely Managing at Least One Crisis», *Gizmodo*, 18/10/2018, buff.ly/2Cr1Qoo. Facebook ha classificato

La seconda misura sarebbe lo spaccettamento – con una legislazione anti-trust – dei Gafa, che li costringerebbe a scegliere tra Google e YouTube, Facebook e Whatsapp eccetera. Per quanto riguarda le *fake news*, ciò ridurrebbe o complicherebbe la possibilità di campagne multicanale condotte attraverso il profilo di un unico utente.

A rendere improbabile l'approvazione di provvedimenti di questo tipo non c'è solo la tradizionale allergia dell'americano medio e del suo parlamentare verso la regolamentazione dell'economia. C'è anche la Cina, la cui ascesa online è più impetuosa di quella offline. Ridurre la taglia delle principali aziende americane del settore vuol dire indebolirle nella competizione per il predominio mondiale del controllo dei dati. Il problema non si porrebbe nel mercato interno, dove l'attrattiva di social network allogeni sarebbe confinata alle minoranze etniche, ma nel resto del mondo – che, come dice l'ex amministratore delegato di Google, va verso la divisione in due di Internet, uno guidato dagli Usa e uno dalla Cina¹⁹. Proprio lo spauracchio della disinformazione, ora agitato da chiunque voglia delegittimare un avversario politico (o mediatico), sta fornendo a governi più o meno liberali l'occasione a lungo attesa di regolamentare la Rete.

Non avrebbe senso per Washington favorire indirettamente Pechino, visto che quest'ultima può già sfruttare un certo *idem sentire* con i regimi dittatoriali tradizionalmente fuori dall'influenza culturale ed economica anglo-americana. Per competere con i loro equivalenti cinesi, i Gafa e Amazon hanno bisogno di quella quantità enorme di dati cui solo la loro attuale posizione semi-monopolistica permette di accedere.

Sono passati due anni dall'esplosione dello scandalo *fake news*. La Russia è il villano di sempre agli occhi degli Stati Uniti. Trump è ancora presidente. Internet si sta frammentando. La Silicon Valley ha perso quel po' di innocenza che le era rimasta dopo le rivelazioni di Edward Snowden ed è chiamata a chiarire il suo ruolo nel sistema statunitense. I giganti digitali dovranno accettare le logiche analogiche (qui come metafora di «antico») del potere, rinunciando almeno in parte alle illusioni libertarie, planetarie e palingenetiche che pure hanno alimentato la fase iniziale del loro sviluppo. Lo scontro tra Usa e Cina si deciderà anche sulla Rete e Washington si aspetta dai Gafa che la scelta di campo sia netta.

Quanto alla disinformazione, nessun algoritmo è stato né sarà mai in grado di individuarla ed eliminarla. La psicosi da *fake news* potrebbe però avere il merito di incentivare una riflessione sul ruolo che stanno assumendo nelle nostre vite i dati e chi li controlla. Un problema culturale prima che geopolitico, la cui soluzione non si trova su nessun motore di ricerca.


come politici e rimosso alcuni post sponsorizzati che in realtà non si occupavano di politica, ma utilizzavano alcune parole chiave come «latino», «afroamericano», «messicano», «donne», «Lgbt» o erano semplicemente scritti in lingua spagnola. Naturalmente il social network non ha divulgato le linee guida cui si dovrebbero attenere gli algoritmi e i moderatori in carne e ossa. J. GUYNN, «Facebook Labels African-American, Hispanic, Mexican Ads as Political», *Usa Today*, 18/10/2018, buff.ly/2Re91EK

19. L. KOLODNY, «Former Google CEO Predicts the Internet Will Split in Two – And One Part Will Be Led by China», *CNBC*, 20/9/2018, goo.gl/avC4MT

LA STRATEGIA DEL CUCULO I GIGANTI DIGITALI VOGLIONO PRENDERSI TUTTO

I padroni della Rete tra alleanze, divisioni e linee di frattura. Il dominio Usa, la sfida cinese, la guerriglia russa. Il (velleitario?) tentativo dell'Ue di costringere Google, Apple, Facebook e Amazon a piegarsi alle regole comunitarie.

di Francesco VITALI GENTILINI

1.  A STORIA DELLA GEOPOLITICA CI INSEGNA che il diritto, soprattutto in campo internazionale, è dettato dai più forti e rappresenta così la traduzione scritta delle consuetudini imposte sul campo. Eppure l'Unione Europea – proprio nell'anno in cui appare più debole, stretta nella tenaglia russo-americana e dilaniata al suo interno da forze centrifughe neonazionaliste – ha azzardato una proiezione di potenza nel campo da cui si domina l'economia mondiale, quello dei dati. Dopo un lungo e travagliato percorso, il 25 maggio 2018 è infatti diventato applicabile il nuovo regolamento Ue in materia di protezione dei dati personali (Gdpr)¹ che, tra l'altro, impone alle società straniere, ovunque si trovino, di adeguarsi alla normativa europea nel caso in cui offrano beni e servizi a persone ubicate nel territorio dell'Unione. A questo esercizio di potenza, diretto soprattutto verso Usa e Cina, non si erano opposti né Regno Unito pre-Brexit né Irlanda – pur così soggetta alle potenti lobby dell'industria digitale americana. È una sfida ai giganti della Rete condotta non sul campo dell'economia e dell'innovazione, ma del diritto, giocando sulla massa critica dei paesi europei per una volta uniti.

La sfida europea nel campo digitale si sarebbe dovuta completare, sempre nel 2018, con l'approvazione di altre due normative con proiezione extra Ue: il rego-

1. Il regolamento Ue 679/2016, meglio noto come Gdpr, è entrato in vigore il 24 maggio 2016, ma è applicabile (quindi effettivo) solo dal 25 maggio 2018. Chi non rispetta il regolamento, ovunque si trovi, può essere soggetto a ingenti sanzioni pecuniarie che possono arrivare al 4% del fatturato globale. Rimane tutta da verificare la capacità europea di andare fino in fondo nel processo di imposizione della normativa, nonché di incassare effettivamente sanzioni comminate a societàlocate al di fuori del territorio Ue.

lamento ePrivacy² e la nuova normativa in materia di copyright³. Ma le multinazionali del settore non hanno subito passivamente e, sostenute dai propri governi, hanno prima fatto «aggiustare», come nel caso del Gdpr, i testi di legge e poi hanno ottenuto di rinviarne l'approvazione definitiva.

I principali antagonisti (saltuariamente alleati) del sistema europeo appaiono gli stessi da molti anni: sono i cosiddetti «Gafa»: Google, Apple, Facebook, Amazon. Ma in realtà, nel tempo, hanno cambiato natura e conquistato nuovi territori. Google è diventato una sussidiaria di Alphabet e da motore di ricerca ha invaso i settori della sanità, della difesa, dei pagamenti, dell'editoria, delle scienze applicate, del trasporto, solo per citarne alcuni. Simile la strategia di Apple nel suo «piccolo» ma solido recinto dorato. Facebook, di cui i detrattori hanno citato il leggero calo di crescita, ha investito in società divenute leader indiscusse, ossia Instagram e WhatsApp, strumenti indispensabili di comunicazione, di lavoro, di monitoraggio. Amazon, spesso conosciuta solo per aver spazzato via pezzo a pezzo i negozi tradizionali e il mondo della grande distribuzione, è in realtà anche uno dei più importanti leader nel campo del *cloud computing* e dei servizi avanzati ambiti dall'industria di ogni settore, a partire da quella della difesa. Difatti, quelli che prima erano conosciuti come i «big della Rete»⁴, sono ora chiamati i «giganti digitali».

2. Per arrivare a questo punto, i giganti digitali hanno quasi tutti seguito con successo l'efficace strategia adottata da Google, che imita quella del cuculo⁵. Questo uccello depone il suo uovo nel nido di altre specie. L'uovo invasore è simile a quelli della specie ospitante, così il proprietario del nido se ne prende cura come se fosse suo. Dopo la nascita, però, l'uccellino del cuculo cresce molto più velocemente degli altri pulcini e, quando è abbastanza grande, butta giù dal nido i piccoli antagonisti, occupandone il posto. Nel mondo digitale il sistema è un po' più complesso. I Gafa, una volta scelto il settore, offrono servizi gratuiti o quasi alle imprese del mercato di interesse consentendo loro, nel breve periodo, di abbassare i costi e migliorare la produttività. Nel frattempo, assorbono dati, competenze, clienti, fino a diventare improvvisamente più grandi ed efficienti di tutti gli operatori di cui erano partner.

2. La proposta di regolamento si applica a tutti i fornitori di comunicazioni elettroniche, superando la direttiva ePrivacy (2002/58/CE). Le misure previste ambiscono a sostenere il mercato unico digitale europeo rendendo, al tempo stesso, più efficace la tutela dei dati personali degli utenti. Dovrebbe portare, tra l'altro, al superamento della famigerata normativa sui *cookies* che obbligava semplicemente le imprese a informare gli utenti (tramiti fastidiosi pop up) in merito all'utilizzo di agenti traccianti, senza garantire, di fatto, alcuna tutela effettiva contro attività di monitoraggio.

3. L'attuale versione approvata in bozza dal Parlamento europeo ha generato forti tensioni tra il mondo editoriale e le associazioni per le libertà digitali, sostenute anche da Google & Co. Una delle maggiori contestazioni riguarda il potenziale potere di censura che si rischia di attribuire involontariamente proprio ai giganti digitali, mediatori ultimi dell'informazione.

4. In campo tecnico erano classificati come Ott (Over-the-top), ovvero i fornitori di servizi aggiuntivi sopra la Rete, anche per distinguere il ruolo dalle società di telecomunicazioni.

5. F. VITALI, «Mobile Payment e identità elettronica: le nuove sfide per la supremazia commerciale e politica», *Nomos & Khaos*, Rapporto Nomisma 2012-2013 sulle prospettive economico-strategiche – Osservatorio scenari strategici e di sicurezza, 2013, pp. 311-324.

Una parte del settore bancario europeo potrebbe seguire questo destino. Da anni, ormai, i Gafa hanno prima cercato partnership con attori del settore dei pagamenti per poter tracciare gli acquisti offline, conquistando l'accesso alle principali banche dati del settore, cercando accordi diretti – di marketing e commerciali – con i gestori delle carte di credito e con gli istituti bancari. Hanno così sviluppato forme alternative di pagamento tramite app come Apple Pay, Google Pay o Amazon Pay, offrendosi come mediatori tra gli utenti e gli istituti di credito nelle operazioni di acquisto o negli scambi di denaro P2P⁶. Nel frattempo hanno rotto il fronte delle banche, indecise se arroccarsi o se tentare di collaborare, disposte a dividere parte delle commissioni pur di accedere a un maggior numero di clienti potenziali. I giganti digitali non sono però interessati a guadagnare percentuali di commissione, la loro strategia è accedere ai dati delle transazioni, per poi prendersi tutto il piatto. Ma per completare il percorso avevano bisogno di entrare in un settore fortemente regolamentato, senza i vincoli delle banche. E ci sono riusciti sfruttando in chiave geoeconomica un'altra norma europea, la cosiddetta direttiva PSD2⁷ sui servizi di pagamento nel mercato interno, pensata per modernizzare e aprire alla concorrenza l'asfittico mondo bancario europeo.

Dal 2019, con il perfezionamento del quadro normativo che consente l'attuazione della direttiva a livello nazionale, molti nuovi fornitori di servizi, start-up, telco e, soprattutto, i Gafa, potranno accedere e gestire direttamente operazioni sui conti correnti dei clienti delle banche⁸, raccogliere senza mediatori quei dati necessari a completare il profilo degli utenti e offrire loro nuovi prodotti e servizi, operando in accordo con gli istituti di credito o scavalcandoli quando più remunerativo. Il settore bancario non è rimasto a guardare. Sono nate anche nuove iniziative come la Cbi Globe, una piattaforma digitale sviluppata dal Consorzio interbancario Cbi e da Nexi, che difficilmente potranno però reggere l'urto del cuculo nel momento in cui deciderà di conquistare il nido. Al consumatore europeo probabilmente non resterà alternativa che passare da un oligopolio nazionale inefficiente a un oligopolio straniero decisamente migliore nel generare e intascare utili. Un assalto guidato in partnership con grandi gruppi finanziari americani, anche se ancora indecisi tra l'essere alleati, antagonisti o comproprietari dei giganti digitali. Due esempi: il supporto offerto da gruppi come JP Morgan; le aspre critiche contro Facebook e Google espresse pubblicamente da George Soros⁹, prima dello scoppio dello scandalo di Cambridge Analytica.

6. *Peer to peer*. Sono gli scambi diretti tra utente e utente, come il passaggio di denaro elettronico tra amici o familiari.

7. La direttiva 2015/2366/UE sui servizi di pagamento nel mercato interno, teoricamente, è stata scritta per aprire alla concorrenza il settore dei pagamenti al dettaglio, rendendolo più sicuro ed efficiente, sostenendo l'innovazione e aumentando il livello di sicurezza dei servizi di pagamento elettronici.

8. La direttiva apre il mondo bancario al fondamentale ruolo dei cosiddetti Tpp (Third Party Payment Services Provider), gli Aisp (Account Information Service Provider) e i Pisp (Payment Initiation Service Provider).

9. Lo scorso 25 gennaio 2018, in occasione del World Economic Forum tenutosi a Davos, il finanziere americano di origine ungherese ha attaccato frontalmente Google e Facebook, affermando che le loro dimensioni li hanno resi di fatto «ostacoli all'innovazione», che il loro comportamento «monopo-

Il modello di attacco dei giganti digitali è replicabile in molti altri settori. Basti pensare al rischio immediato che corre il Gruppo Ferrovie dello Stato Italiane nel rendere disponibili gli orari dei treni a Google, consentendone l'integrazione nel mondo degli *smart devices*, e quindi all'interno dell'ecosistema controllato dalla società americana. Questa scelta è di certo utile per i viaggiatori, rendendo più facile e veloce selezionare modalità e tempi di trasporto; non costa nulla a Fs nel breve periodo, ma consente alla *corporation* americana di cominciare a conoscere e ad anticipare le scelte dei clienti di Trenitalia molto meglio di Trenitalia stessa. Tale modello reggerà finché Google non deciderà che esistono marginalità tali da spingerla a diventare la piattaforma per gestire i viaggi degli italiani o del resto dei cittadini europei al posto degli altri operatori sul mercato. È un rischio comunque minore rispetto a quello che già stanno affrontando le case automobilistiche europee (e non solo) di fronte alle sfide poste dagli sviluppi della guida autonoma (Google in testa) e da cambi di scenario come quelli imposti da società di servizi come Uber¹⁰. La situazione è tale che lo stesso gruppo Daimler starebbe completamente ridefinendo il proprio ruolo da mero produttore automobilistico a fornitore di servizi nei prossimi anni.

La sfida dei «cuculi digitali» è diventata aspra anche nel settore sanitario che, nel medio termine, si dimostrerà forse il più redditizio di tutti. La conquista dei dati sulla salute delle persone è però più complessa, forse perché più tutelata e, comunque, ancora protetta dal maggior desiderio di riservatezza delle persone interessate. Accedere alla conoscenza dei dati sanitari della popolazione significa poter attingere contemporaneamente alla ricchezza delle società assicurative e a quella delle case farmaceutiche, moltiplicandone poi i potenziali profitti sulle prestazioni offerte. Oltre ai Gafa, cercano l'assalto a questo settore altri vecchi giganti, come Ibm, che non ha ancora accesso a quantità di dati analoghe a quelle dei concorrenti, ma che può competere sul fronte delle tecnologie per il trattamento dei dati, in particolare tramite l'uso di sistemi avanzati di intelligenza artificiale, come Watson. Proprio in questo settore c'è uno scontro sottotraccia tra *corporations* americane, che negli ultimi due anni hanno identificato anche l'Italia tra le potenziali terre da conquistare a basso costo.

3. Su scala globale, esistono pochissime imprese in grado di contendere parte del mercato ai giganti digitali statunitensi. Tra esse vi sono alcune piccole eccellenze israeliane e società del Lontano Oriente, come quelle coreane¹¹. La Russia, non

listico» li ha resi una concreta «minaccia» per la società, anche se la loro supremazia ha i giorni contati. A suo avviso sarebbe solo una questione di tempo prima che si rompa il dominio globale dei monopoli statunitensi sulle tecnologie dell'informazione. Vedi ad esempio goo.gl/obw3HZ

10. Secondo Bloomberg, Uber starebbe chiudendo l'accordo con Morgan Stanley e Goldman Sachs per quotare il titolo in Borsa, con una valutazione per un'offerta pubblica iniziale di 120 miliardi di dollari. Vedi A. BARINKA, E. NEWCOMER, «Uber Valued at \$120 Billion in an IPO? Maybe», 17/10/2018, www.bloomberg.com

11. Samsung, ad esempio, ha cercato di costruire una sorta di ecosistema stile Apple, sviluppando tecnologie e applicativi proprietari come Samsung Pay. Tali tentativi appaiono però, al momento, velleitari, relegando la multinazionale sudcoreana a un secondo livello, in quanto si basano su servizi comunque mediati da Google tramite il sistema operativo Android.

essendo assolutamente in grado di competere a livello strategico, rimane sul campo con una sorta di guerriglia asimmetrica, nella speranza di recuperare saltuariamente il proprio gap in settori specifici dell'universo digitale. L'unico paese – o meglio, continente – in grado di impensierire gli americani nel medio termine è quello cinese.

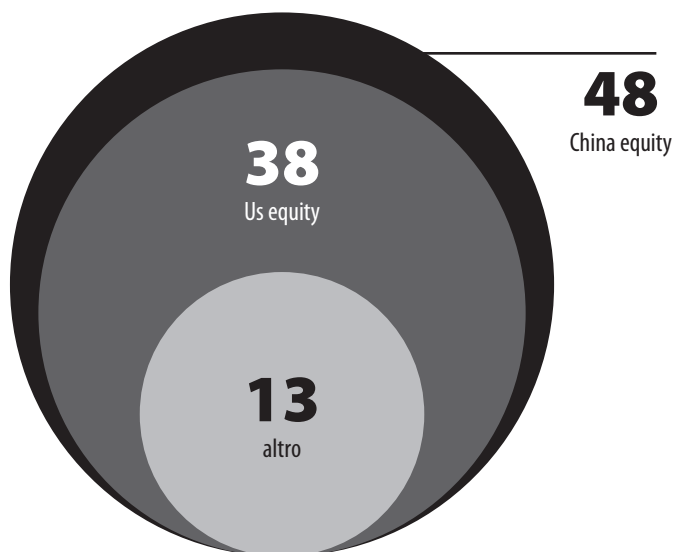
La strategia cinese si è sviluppata su vari assi, tutti pensati in chiave strategica per poter fare un balzo tecnologico militare nei prossimi dieci-quindici anni. Internamente ha consentito uno sviluppo dopato dal dirigismo statale e dall'assenza di concorrenza a compagnie nazionali di dimensioni paragonabili a quelle americane, in testa a esse le famose Bat: Baidu, Alibaba, Tencent. Le uniche società al mondo che hanno potuto sfruttare economie di scala paragonabili a quelle statunitensi, ma autonome dalla gabbia dorata offerta da Alphabet. Società tecnologiche come Huawei, Zte, Xiaomi e tante altre hanno invece cercato con successo la strada esterna proponendosi sia come leader nel mercato *consumer* sia come partner indispensabili delle principali società di telecomunicazioni al mondo. Le società cinesi hanno sfruttato l'orizzonte dei risultati di breve termine – e quindi la logica del risparmio immediato che attrae i governi e le imprese occidentali – come cavallo di Troia per disseminare i propri sensori ovunque. Forniture di *devices* e di componentistica specializzata vengono offerte da anni anche sottocosto – e comunque al di fuori delle regole di produzione occidentali – pur di essere indispensabili. Chip che trasmettono lecitamente o illecitamente¹² i propri dati in «madrepatria», una terra che non corrisponde però con quella del luogo di acquisto. In Italia, così come in tanti altri paesi europei, non esiste compagnia di telecomunicazioni che non utilizzi su ampia scala tecnologia cinese, oppure non sia addirittura partecipata o controllata dai partner orientali. A nulla, in tale senso, sono valse gli allarmi – sicuramente interessati da un punto di vista strategico ma anche commerciale – del governo e dei servizi segreti americani.

Il Dragone, da buon pianificatore, al fine di ridurre il gap tecnologico, economico e militare che lo separa dagli Stati Uniti non si è limitato a queste due linee strategiche o ad attacchi hacker puntuali per «acquisire» segreti occidentali. Ha deciso di sfidare l'Occidente investendo pesantemente in ricerca nei settori strategici avveniristici, come alcune applicazioni tecnologiche della fisica quantistica, e strumenti fondamentali per lo sfruttamento dei big data, come l'intelligenza artificiale. Proprio in questo campo la Cina ha concentrato una quota ingente delle sue risorse, superando già nel 2017 il livello di investimenti americani (*grafico 1*)¹³. Anche solo questo trend nel settore porterà la Cina, in pochi anni, ad avere un incremento del prodotto interno lordo quasi doppio a quello statunitense (*grafico 2*)¹⁴.

12. J. ROBERTSON, M. RILEY, «The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies», 4/10/2018, www.bloomberg.com. Cfr. J. ROBERTSON, «The Big Hack Amazon, Apple, Supermicro, and Beijing Respond», 4/10/2018, www.bloomberg.com

13. «The State of Artificial Intelligence 2018», CB Insights, 2018. Cfr. J. VINCENT, «China Overtakes US in AI Startup Funding with a Focus on Facial Recognition and Chips», *The Verge*, 22/2/2018.

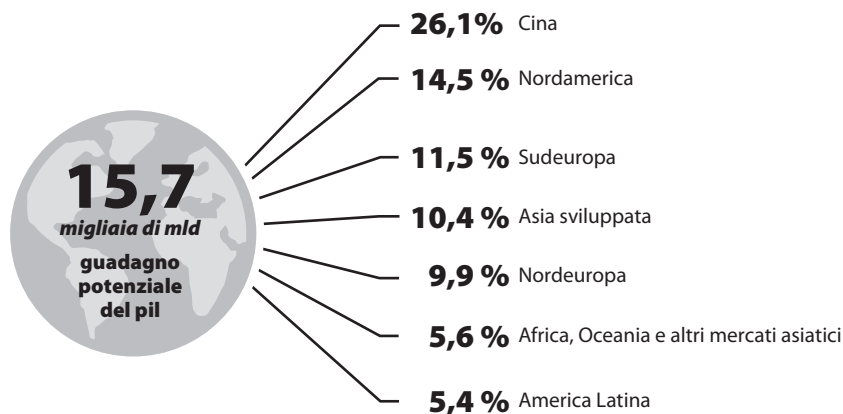
14. «2018 AI Predictions 8 Insights to Shape Business Strategy», *PwC*, 2018.

Grafico 1 - FINANZIAMENTI ALLE START-UP DI AI, 2017 (valori %)

Fonte: «The State of Artificial Intelligence 2018», CB Insights, 2018

In questa sfida globale non bisogna dimenticare che il confronto finale non è tra economie, ma tra modelli di società, di democrazia, di governo. Semplicemente: di vita. E la sfida più seria, in questo campo, non è portata dai cinesi, ma dagli stessi giganti digitali statunitensi, a partire da Facebook. Non si sono ancora chiuse le molteplici inchieste avviate dal Senato e da altre istituzioni americane, così come da varie controparti europee, sulle operazioni di manipolazione sociale dell'elettorato americano, realizzate tramite Facebook e altri social media durante la competizione in cui è stato eletto il presidente Donald Trump. I documenti sino ad ora pubblicati hanno confermato l'esistenza di operazioni sociali – una volta definite di guerra psicologica, ora derubricate a marketing politico – volte a modificare segretamente le scelte dell'elettorato. Tali operazioni spaventano tutte le parti politiche in campo, incluse quelle che ne hanno beneficiato. Tutti, infatti, sono soggetti all'unico reale potere di controllo (o azione attiva) esercitato dai gestori delle piattaforme di comunicazione sociale. Anche nello scandalo relativo a Cambridge Analytica, quasi tutti gli studi sino ad ora si sono concentrati sulla punta dell'iceberg – ovvero sulle attività di raccolta, elaborazione e manipolazione dei dati condotti da una piccola «terza parte».

Per capire e analizzare quello che avviene in forma macro all'interno del mondo dei Gafa e dei Bat occorre però interrogarsi sul potere che risiede a monte del caso Cambridge Analytica e di tutto questo processo di potenziale manipolazione

Grafico 2 - PREVISIONI - IMPATTO DELL'AI SUL PIL NEL 2030

Fonte: PwC Global Artificial Intelligence Study, 2017

sociale, come ad esempio quello garantito, nel caso di Facebook, dal suo algoritmo di newsfeed¹⁵ o da quello che gestisce la profilazione puntuale dei suoi iscritti per finalità di marketing. Senza una sorta di trasparenza¹⁶ algoritmica – che renda espliciti all'utente i dati utilizzati e i principi puntuali che ne governano il funzionamento, indipendentemente dalla società e dallo Stato coinvolto – la capacità del cittadino di esprimersi compiutamente in democrazia sarà comunque compromessa.

L'elemento quotidiano – il dato puntuale sulle proprie attività, sulle scelte o sulla salute – nell'era digitale dell'IoE (*Internet of Everything*) assurge così a valore strategico nella competizione internazionale. Proprio per questo motivo l'applicazione extra Ue del Gdpr – unita a una più costante e incisiva azione dell'antitrust europeo – sarebbe potuta essere un ottimo strumento per limitare lo strapotere dei giganti digitali, a patto di avere la capacità di imporre il rispetto della legge, che

15. Si veda, ad esempio, l'importante progetto di analisi dell'algoritmo di *newsfeed* di Facebook – facebook.tracking.exposed, Fbtrex – condotto anche in Italia durante la campagna elettorale 2018; C. AGOSTI, E. ARGREAVES ET AL., «Fairness in Online Social Network Timelines: Measurements, Models and Mechanism Design», paper, International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI 2018), Barcellona, Spagna, 28-31/8/2018; F. CHIUSI, C. AGOSTI, «The Influence Industry – Personal Data and Political Influence in Italy», *Tacticaltech*, giugno 2018, goo.gl/gDrcmY

16. Il tema della trasparenza algoritmica è di complessa soluzione. Si scontra innanzitutto con la necessità di tutelare la proprietà industriale e intellettuale che sta alla base del successo di un'impresa digitale, ma anche con l'oggettiva difficoltà di definire chiaramente le logiche di funzionamento di determinati algoritmi, come quelli basati sulle reti neurali. L'ostacolo più significativo, però, è posto proprio dal desiderio delle società proprietarie degli algoritmi di continuare ad avere totale libertà di azione nel loro operato senza dover risponderne a nessuno – siano essi gli utenti o le autorità preposte – di *bias* statistici volontari o involontari, di forme di discriminazione o di manipolazione sociale, di abusi o di manipolazioni di mercato. Cfr. F. VITALI GENTILINI, «Il lato oscuro degli algoritmi e dei loro padroni», *Limes*, «Chi comanda il mondo», n. 2, 2017, pp. 213-220; A. LAFRANCE, «Not Even the People Who Write Algorithms Really Know How They Work», *The Atlantic*, 18/9/2015, www.theatlantic.com

d'altra parte era nell'interesse di tutti gli Stati membri Ue prima del voto inglese pro Brexit. In questa distopia tecnologica¹⁷, incuranti della propria riservatezza e delle sfide geoeconomiche poste alla difesa degli interessi nazionali, i corpi e le case dei cittadini europei continuano ad accogliere gadget connessi, tra cui – solo per fare un esempio – i cosiddetti «speaker (altoparlanti) intelligenti», adesso rinominati «maggior domi elettronici», che sarebbe però più opportuno definire «microfoni direzionali con sistema remoto di registrazione e analisi delle conversazioni casalinghe» per finalità non verificabili. Sistemi del tutto simili, comunque, a quelli abbinati alle più recenti smart tv, ai telefoni cellulari dotati di intelligenza artificiale (anch'essa a distanza) e di un numero indeterminato di altri apparati elettronici. Sono ottimi strumenti per monitorare e classificare le tribù elettorali americane¹⁸, così come quelle di ogni altro paese. Il gigante digitale a cui dobbiamo prestare attenzione è dentro di noi.

17. F. VITALI, «Geopolitica del “selfie”: nuovi strumenti per orientare politica ed economia mondiale», *Nomos & Kbaos*, Rapporto Nomisma 2013-2014, Agra, Roma 2014, pp. 289-304.

18. S. HAWKINS, D. YUDKIN ET ALII, «Hidden Tribes: A Study of America's Polarized Landscape», *More in Common*, 2018.

WASHINGTON E SILICON VALLEY NON SI AMANO MA SPIANO IL MONDO INSIEME

di Luca MAINOLDI

Pentagono e intelligence hanno attivamente contribuito alla nascita dei giganti americani della Rete. E da anni ne utilizzano tecnologie e dati per studiare le tendenze globali. Nonostante la sbandierata ritrosia delle multinazionali hi-tech.



L DOMINIO INFORMATIVO GLOBALE

1.

statunitense deriva dalla complessa interazione tra la comunità d'intelligence federale e i giganti della Rete, noti comunemente come Gafa (Google, Apple, Facebook, Amazon), ai quali si aggiungono aziende mature come Microsoft e società dell'economia immateriale come eBay, PayPal, Airbnb eccetera.

I dati raccolti dalle imprese americane sono di gran lunga superiori a quelli captati dalla Nsa, al punto che l'ex direttore dell'Agenzia con sede a Fort Meade (e della Cia) Michael Hayden ha potuto affermare ironicamente che esiste un'entità che «raccolge i vostri messaggi di testo, la vostra navigazione sul Web, ogni ricerca che avete fatto! Indovinate chi è? È Google. Non è l'Nsa».

Poiché l'80% dei dati personali dell'umanità sono detenuti dai Gafa che li utilizzano a fini commerciali¹, cosa accadrebbe se ad esempio Google fosse un vero servizio di spionaggio? Se lo sono chiedi il sito d'informazione francese Zone d'Intérêt e il blog Electrospace², per i quali il possesso di mail e messaggi di centinaia di milioni di persone (425 milioni di utenti attivi di Gmail nel 2012, più quelli di Hangouts) significa che Google dispone di un accesso privilegiato alle telecomunicazioni mondiali, «al punto da agire come una grande agenzia Comint, non diversa dall'Nsa o da Gchq (l'intelligence britannica addetta allo studio delle telecomunicazioni, *n.d.r.*)». «Le informazioni contenute nei server della società, se sfruttate tramite programmi di analisi comportamentale e selezionate secondo parametri precisi, andrebbero a costituire una potente banca dati a fini d'intelligence».

Questo senza contare gli ulteriori servizi offerti da Google – da Earth a Street View – creati combinando immagini satellitari e le riprese effettuate al suolo dalle

1. Cfr. M. DUGAN, CH. LABBÉ, *L'homme nu*, Paris 2016, Robert Laffont p. 23.

2. «What if Google Was an Intelligence Agency?» *Zone d'Intérêt*, 5/8/2014, goo.gl/uJnMQ5

auto della multinazionale in gran parte del mondo. Vetture che hanno anche map-pato le connessioni wi-fi nelle zone attraversate. Per non parlare degli oltre due miliardi di smartphone che usano il sistema operativo Android e degli 800 milioni di utenti che conservano i loro file su Google Drive. Facebook a sua volta raccoglie i dati di 2,3 miliardi di utenti ed è in grado di monitorare anche coloro che non sono iscritti, tramite le pagine Web che mostrano il pulsante *I like*.

È ovvio che le informazioni conservate nei capienti server dei Gafa e dei loro epigoni facciano gola alla Nsa, che da tempo ha avviato il programma Prism. Si tratta di una serie sistemi (Pinwale, Nucleon eccetera) per gestire, attraverso una procedura legale, le informazioni ottenute dai server di almeno nove grandi aziende americane: Microsoft-Hotmail; Google; Yahoo!; Facebook; Paltalk; YouTube; Skype; Aol e Apple.

2. Prism risale al 2007 ma i legami intessuti tra Pentagono, intelligence e aziende del comparto It sono molto più antichi e profondi. Una parte dei fondi semina-li (*seed money*) che ha permesso la nascita di alcuni dei Gafa proviene da enti governativi legati al dipartimento della Difesa e/o alla Cia, in maniera diretta o attraverso società di consulenza che fungevano da intermediari. Già nel 1999 la Délégation des Affaires Stratégiques, il centro d'analisi strategica della Difesa francese, aveva pubblicato un rapporto secondo il quale l'Nsa aveva contribuito alla nascita di Microsoft e che esperti dell'Agenzia figurano tuttora tra gli sviluppatori della società.

Alla fine degli anni Settanta Microsoft sarebbe stata preferita ad Apple perché l'azienda di Cupertino incarnava lo spirito della controcultura dei campus californiani, al punto che i primi Apple I e Apple II avevano accluso nella loro licenza d'utilizzazione il divieto di utilizzo nel settore nucleare, in particolare in quello militare³. Uno spirito libertario che ritroveremo a distanza di trent'anni, quando la *Mela morsicata* si rifiuterà di aiutare l'Fbi a sbloccare lo iPhone di Syed Rizwan Farook, il terrorista pakistano che il 2 dicembre 2015, insieme alla moglie, ha compiuto la strage di San Bernardino. Alla fine il Bureau riuscì a sbloccare il telefono rivolgendosi a una società specializzata, forse israeliana⁴.

I Gafa sono eredi della cultura libertaria dei campus universitari americani, specie californiani, ma sono pure tributari dei rapporti intessuti da decenni tra il mondo accademico, l'industria, il Pentagono e la Cia. Nel 1957 il lancio sovietico dello Sputnik causò in America un notevole shock. Un anno dopo fu fondata la Nasa, ma anche la Darpa (l'Agenzia per i programmi avanzati di ricerca della Difesa) e la Mitre Corporation, un'istituzione non profit governativa, originariamente nata per coordinare gli enti e le aziende che stavano realizzando Sage, il primo programma computerizzato di difesa aerea del mondo.

Dopo lo Sputnik, Cia e Pentagono intensificarono la loro collaborazione con alcune delle più prestigiose università americane, come il Mit e la Stanford Univer-

3. Cfr. F. LEROY, *Surveillance. Le risque totalitaire*, Arles 2014, Actes Sud, p.143.

4. D.E. SANGER, *The Perfect Weapon*, New York City 2018, Crown, pp. 88-99.

sity⁵. Istituzioni che avrebbero giocato un ruolo importante nella nascita dei giganti del Web. Nel contesto californiano degli anni Sessanta nacquero le prime imprese produttrici di semiconduttori: la Fairchild Semiconductor International e la Intel. Tra le aziende californiane nate in quegli anni c'è pure uno dei maggiori contrattisti dell'Nsa, la Saic a lungo definita «l'Nsa della costa Ovest». Prima che nel 2013 si sdoppiasse in Leidos, vera erede dell'azienda madre, e un'altra società che mantiene la sigla originaria. Da tempo entrambe hanno spostato la loro sede a Reston, in Virginia, nei pressi del Pentagono, della Cia e dell'Nsa.

La Saic, insieme all'altro grande contrattista dell'intelligence, quella Booz Allen Hamilton dove lavorava Edward Snowden, fu tra i partecipanti di un particolare forum di discussione strategica oggetto di una recente inchiesta del giornalista britannico Nafeez Ahmed⁶. Secondo Ahmed buona parte della strategia americana per controllare e influenzare i flussi informativi globali è proprio opera dello Highlands Forum, un oscuro gruppo di studio fondato nel 1994 dall'ufficiale di Marina Richard Patrick O'Neill e successivamente trasformato in un ente di diritto privato. Nel 1989 O'Neill preparò uno studio per il Naval War College, dal titolo «Per una metodologia di gestione delle percezioni». Secondo la sua analisi, i soggetti della manipolazione percettiva sono gli avversari da intimidire, che dovrebbero sentirsi vulnerabili; i potenziali alleati, che dovrebbero percepire come giusta la causa promossa dall'America; la leadership e la popolazione civile statunitensi, che dovrebbero persuadersi della necessità di sostenere i costi della guerra.

Materiale politicamente esplosivo, specie nell'ultimo punto, per cui la dirigenza del Pentagono decise di seppellire il rapporto ma incaricò l'autore di costituire un forum che agisse come «una informale rete interdisciplinare, sponsorizzata dal governo federale e focalizzata su informazione, scienza e tecnologia».

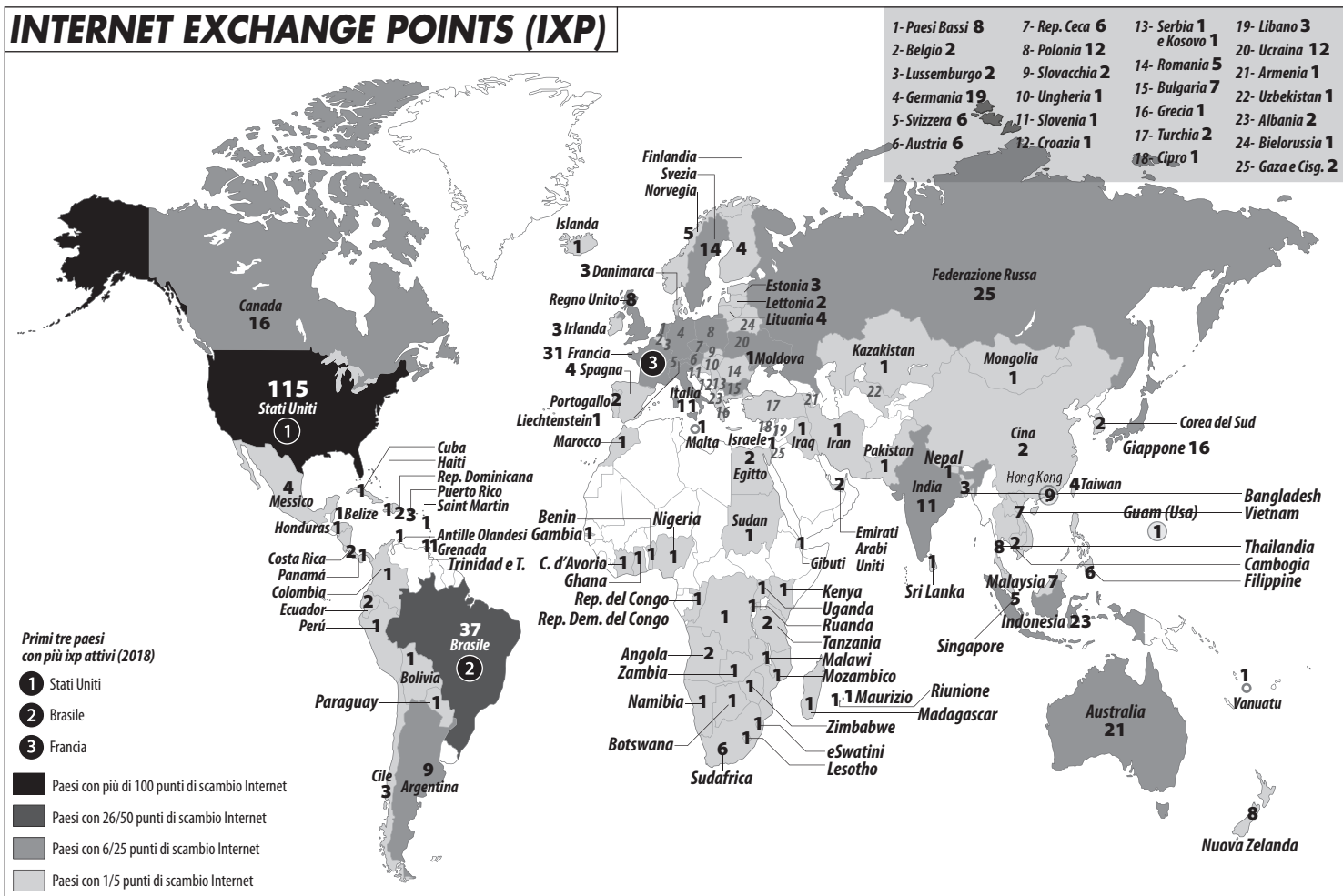
Quindi il vero cervello dell'Highlands Forum sarebbe diventato Andrew Marshall, detto Yoda, dal 1973 al 2015 a capo dell'Office of Net Assessment (Ona), il centro di analisi interno al Pentagono incaricato di delineare strategie a lungo termine. Nel 2001 lo stesso O'Neill ha ammesso che Marshall era di fatto copresidente dell'Highlands Group, assieme a lui e a Anthony J. Tether, all'epoca direttore della Darpa.

Col tempo l'Highlands Forum si è trasformato nell'Highlands Group, una «società di venture capital intellettuale che, grazie alla sua estesa competenza, assiste aziende, organizzazioni e capi di governo». Mentre gli incontri informali organizzati da O'Neill hanno coinvolto rappresentanti delle maggiori aziende tecnologiche americane. Tra queste: Saic, Booz Allen Hamilton, Cisco, Human Genome Sciences, eBay, PayPal, Ibm, Google, Microsoft, AT&T, General Electric. Cui vanno aggiunti i principali media statunitensi. Nulla di nuovo, se si pensa che da diversi

5. Già nel 1946 l'Università di Stanford creò lo Stanford Research Institute, poi diventato nel 1970 lo SRI International, un ente di ricerca che riceve numerosi contratti dal Pentagono.

6. L'inchiesta è divisa in due parti, rispettivamente intitolate: «How the CIA made Google» e «Why Google made the NSA».

INTERNET EXCHANGE POINTS (IXP)



WASHINGTON E SILICON VALLEY NON SI AMANO MA SPIANO IL MONDO INSIEME

anni l'Nsa ha stabilito accordi di collaborazione strategica con almeno 80 aziende americane dell'elettronica, della telefonia e dell'ingegneria informatica⁷.

3. Nel 1994, mentre nasceva l'Highlands Forum, due ricercatori della Stanford University, Sergej Brin e Larry Page, stavano realizzando l'applicazione d'indicizzazione delle pagine Web che diverrà poi il cuore di Google, con fondi della Digital Library Initiative, un programma sponsorizzato dalla National Science Foundation, dalla Nasa e dalla Darpa. Sergej Brin teneva aggiornati dei progressi della sua ricerca due scienziati esterni all'università, Bhavani Thuraisingham e Rick Steinheiser della Cia. All'epoca Thuraisingham lavorava per la Mitre Corporation, dove era responsabile per la Massive Digital Data Systems (Mdds), un'iniziativa sponsorizzata da Nsa e Cia che aveva l'obiettivo di promuovere ricerche innovative nel campo delle tecnologie dell'informazione. Tramite la Mitre, alcuni fondi della Mdds sono stati destinati a Stanford per finanziare le ricerche di Brin.

D'altronde fin dagli anni Ottanta l'Università di Stanford svolgeva studi nel campo della gestione delle informazioni e dell'intelligenza artificiale per conto del Pentagono. Nel 1996 il supervisore di Brin, Jeffrey Ullman, partecipò a un progetto sponsorizzato dalla Darpa per aggregare le informazioni sparse nella rete. Proprio le mansioni che svolge oggi il motore di ricerca di Mountain View. Nel settembre 1998 Brin e Page fondarono la loro società e lanciarono Google. Tra gli investitori della neonata azienda vi erano due imprenditori che ancora oggi mantengono stretti rapporti con la Darpa, cui versano 100 mila dollari ciascuno: Andreas Bechtolsheim e David Cheriton. Bechtolsheim, uno degli ospiti dell'Highlands Forum, ha fondato la Sun Microsystems, dopo aver ricevuto fondi proprio dalla Darpa e dalla facoltà di informatica di Stanford per elaborare il progetto della Sun workstation. Invece Cheriton vanta un rapporto di collaborazione ventennale con la Darpa.

Già nel 1999 Google ricevette 25 milioni di dollari di finanziamento azionario raccolti dalle due maggiori società di venture capital della Silicon Valley, Sequoia Capital e Kleiner Perkins Caufield & Byers. Entrambe le aziende sono nate nel 1972 e hanno sede a Menlo Park. In concorrenza tra loro hanno finanziato la maggior parte delle aziende della Valley, tra cui Apple, Google, Oracle, PayPal, YouTube, Instagram, Yahoo! WhatsApp, Amazon, Twitter.

Entrambe le imprese intrattengono importanti rapporti con il Pentagono e il mondo dell'intelligence. In particolare, Kleiner Perkins ha sviluppato una proficua relazione con In-Q-Tel, il fondo d'investimento della Cia per le imprese ad alta tecnologia. Mentre diverse start-up finanziate da Sequoia Capital hanno ricevuto contratti dal Pentagono, soprattutto dopo l'11 settembre quando Mark Kvamme, tra i massimi dirigenti della società, si incontrò con l'allora segretario alla Difesa, Donald Rumsfeld, per discutere dell'uso di tecnologie emergenti in ambito militare e d'intelligence⁸.

7. Cfr. I. RAMONET, *L'Empire de la surveillance*, Paris 2015, Éditions Galilée, p. 84.

8. Cfr. «Fending Off DoJ Subpoena, Google Continues Longstanding Relationship with US Intelligence», *Homeland Security Today*, 26/1/2006.

Proprio In-Q-Tel, creata nel 1999, è strumento essenziale per individuare quelle tecnologie che in futuro potrebbero essere utilizzate dalla comunità d'intelligence statunitense. Tra le prime imprese finanziate da In-Q-Tel vi era Keyhole, società che ha successivamente sviluppato un innovativo sistema di presentazione di mappe ricavate da immagini satellitari. Peraltro Keyhole è la sigla per esteso dei satelliti fotografici realizzati dalla Cia, ovvero KH (Keyhole). Nel 2004 Keyhole fu acquistata da Google, che da allora ne ha impiegato le tecnologie per elaborare Google Earth. Mentre soltanto l'anno prima Google aveva sottoscritto un contratto con la Cia per adattare il suo motore di ricerca alla rete interna dell'Agenzia, la Intelink Management Office.

4. Gli attentati dell'11 settembre 2001 hanno accelerato i programmi di sorveglianza di massa del Pentagono e della comunità d'intelligence. Già due anni prima J. Brian Sharkey, allora vice direttore dell'Ufficio per i sistemi informativi della Darpa, presentò il Total Information Awareness (Tia), un sistema di sistemi in grado di raccogliere informazioni da fonti aperte, come Internet, e da database pubblici e privati, con l'obiettivo di scandagliare i dati raccolti per prevenire potenziali attentati o attività sospette. Inizialmente il progetto fu bellamente ignorato, ma dopo il crollo delle Torri Gemelle fu rilanciato per impulso dell'ammiraglio John Poindexter, ex consigliere per la Sicurezza nazionale con Ronald Reagan, coinvolto nello scandalo Irangate.

Per coordinare i precedenti sforzi nel campo dell'analisi dei dati, nel gennaio 2002 la Darpa creò l'Ufficio per la consapevolezza informativa (Iao) con «il compito di immaginare, sviluppare, applicare, integrare e dimostrare tecnologie dell'informazione, componenti e prototipi di sistemi informativi per affrontare minacce asimmetriche attraverso la consapevolezza totale dell'informazione»⁹. Tra i progetti previsti dall'Iao ce n'era uno rivolto all'analisi delle reti sociali, il Progetto di analisi dei social network scalabili (Ssnap), con l'obiettivo di creare un modello sociale che avesse le stesse caratteristiche dei gruppi terroristici, così da discriminare sul campo questi gruppi da altri tipi di aggregazioni sociali. Il Tia fu bocciato dal Congresso, ma successivamente le rivelazioni di Snowden avrebbero dimostrato come molte delle tecnologie elaborate dall'Nsa si basassero sulla sua filosofia concettuale.

In seguito Poindexter presenziò agli Island Forum, gli incontri organizzati dall'Highlands Group e dal ministero della Difesa di Singapore, cui partecipano i rappresentanti dei Five Eyes, l'alleanza spionistica formata da Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda, e i delegati di Israele, Francia, Svezia, India¹⁰. Nel 2004 Poindexter incontrò Peter Thiel e Alex Karp, fondatori della neonata Palantir, una società che stava realizzando sistemi di raccolta e gestione delle

9. *Report to Congress regarding the Terrorism Information Awareness Program*, 20/5/2003, p. 1.

10. Singapore si conferma uno degli snodi principali dei sistemi di sorveglianza globale a guida americana, anche perché sul suo territorio transitano numerosi cavi intercontinentali di telecomunicazione. Da notare anche la presenza d'Israele, che intrattiene strette relazioni di sicurezza con la città-Stato.

informazioni concettualmente assai simili al Tia. L'ammiraglio permise a Palantir di ottenere lucrosi contratti governativi. E nello stesso anno Thiel conobbe Gilman Louie, fondatore e presidente di In-Q-Tel.

Thiel, che nel 1999 era stato tra i fondatori di PayPal, e Louie avrebbero avuto un ruolo importante nella nascita di Facebook. Il primo con 500 mila dollari fu tra i primi a investire nella creatura di Mark Zuckerberg. Il secondo era socio di James Breyer, capo di Accel Partners, società di venture capital che nel 2005 investì 12,7 milioni di dollari in Facebook. Peraltro Breyer era alla testa della National Venture Capital Association (Nvca), del cui board era membro anche Louie.

Così nel 2008 Facebook raccolse altri 27.5 milioni di dollari tramite Greylock Venture Capital, tra i cui partner figurava Howard Cox, un altro componente dei board di Nvca e di In-Q-Tel. Allora con un investimento totale di 40,2 milioni di dollari, le due società detenevano il 31,65% del capitale di Facebook. «Abbastanza per pesare sulle decisioni del consiglio d'amministrazione»¹¹, afferma Franck Leroy in un saggio sulla sorveglianza di massa.

Per Facebook il salto di qualità finanziario giunse nel 2011, quando Goldman Sachs grazie a una serie d'investimenti portò il valore della società a 50 miliardi di dollari. L'operazione fu guidata da George C. Lee, senior partner della banca d'affari, di cui era chief information officer nella divisione per gli investimenti bancari, e presidente del Global Technology, Media and Telecom Group (Tmt).

In seguito George C. Lee avrebbe partecipato all'Iniziativa per la ciber sicurezza (CySec) del Monterey Institute for International Studies (MiiS), che assieme all'Highlands Forum organizza incontri di studio con l'obiettivo «di esplorare l'impatto della tecnologia sulla sicurezza, sulla pace e sull'uso delle informazioni».

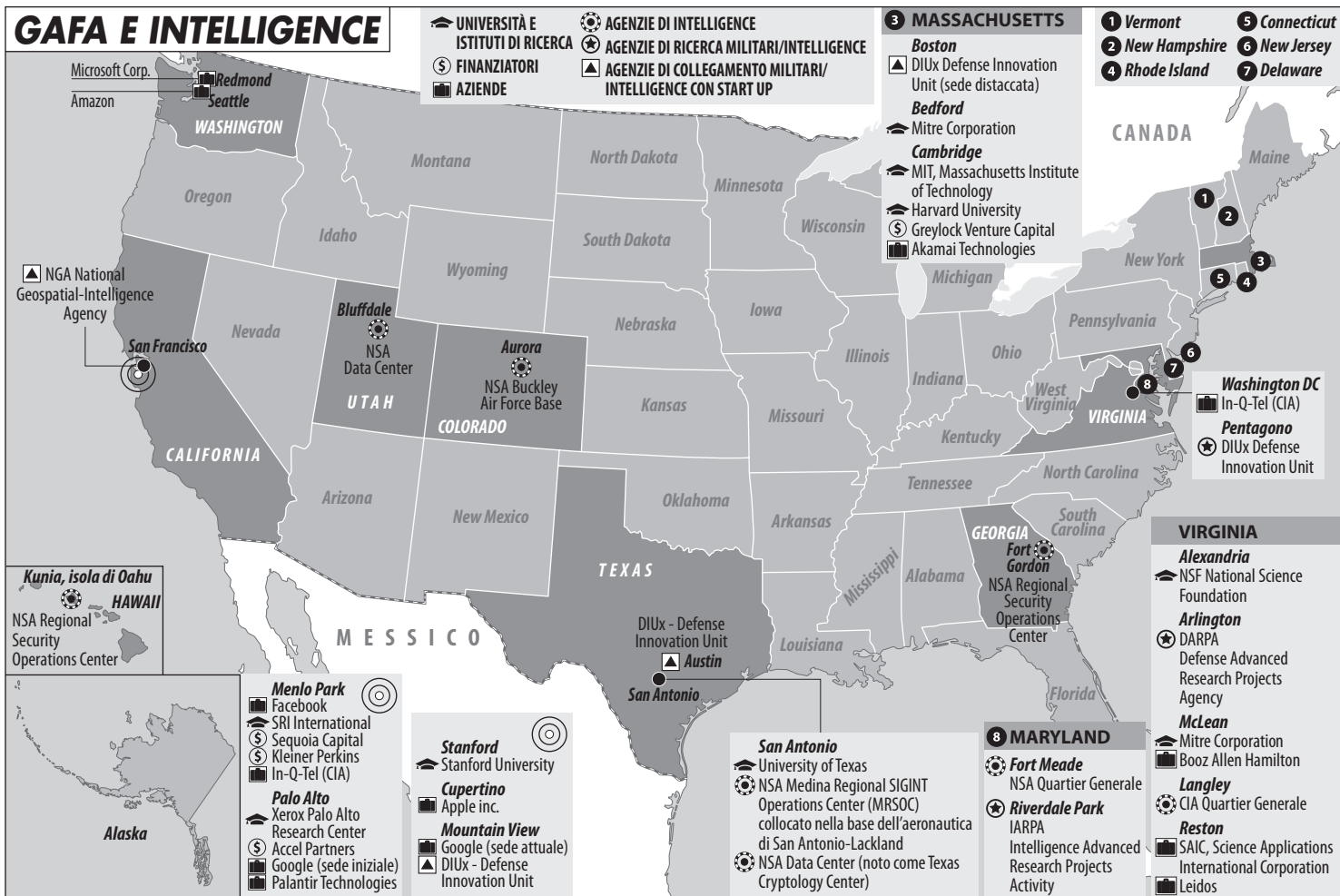
Nel 2011 il superiore di Lee era Stephen Friedman, presidente di Goldman Sachs e membro del board di In-Q-Tel. La banca da lui presieduta ha accompagnato lo sviluppo di altri giganti del Web, come Microsoft, Google ed eBay. E nel 2001 George W. Bush nominò Friedman nel consiglio di intelligence della Casa Bianca, di cui il finanziere diverrà presidente tra il 2005 e il 2009.

Negli ultimi anni i legami tra Google e Pentagono si sono consolidati attraverso contratti che consentono ai militari di sfruttare alcune tecnologie dell'azienda, come Google Earth, e che hanno condotto nella società di Mountain View numerosi dirigenti in precedenza impiegati al dipartimento della Difesa. Tra questi: Michele Weslander Quaid¹², già delegata all'Highlands Forum, diventata chief technology officer di Google dopo aver lasciato l'incarico di consigliere per il sottosegretario alla Difesa per l'intelligence; e Regina Dugan, copresidente dell'Highlands Forum, che nel 2012 si è dimessa dalla Darpa per diventare senior executive di Google e dirigente del suo Gruppo per le tecnologie e i progetti avanzati¹³.

11. F. LEROY, *op. cit.* p. 120.

12. Michele Weslander Quaid ha lavorato in precedenza per la National Geospatial-Intelligence Agency e il National Reconnaissance Office.

13. Nell'aprile 2016 Dugan ha lasciato Google per dirigere il settore di ricerche avanzate di Facebook. Incarico che ha lasciato nell'ottobre 2017.



Secondo il fondatore di WikiLeaks Julian Assange, almeno ai tempi dell'amministrazione Obama la dirigenza di Google svolgeva un ruolo importante nella politica estera americana. Assange menziona dirigenti come Jared Cohen, direttore di Google Ideas, il laboratorio per le ricerche avanzate della società, che è stato consigliere di Condoleezza Rice e di Hillary Clinton quando queste ricoprivano l'incarico di segretario di Stato. Quindi menziona l'ex Ceo di Google Eric Schmidt, che nel 2013 ha realizzato per conto del governo statunitense missioni di diplomazia parallela in Cina, in Myanmar e in Corea del Nord. Peraltro nel 2011 Schmidt e Cohen incontrarono a lungo Assange accompagnati da alcuni funzionari del dipartimento di Stato¹⁴. E nel 2016 Schmidt è stato nominato presidente del neonato Defense Innovation Advisory Board, il cui scopo è applicare all'ambito militare le pratiche e le capacità innovative della Silicon Valley.

5. A partire dal 2013 le rivelazioni di Snowden hanno costretto Google e gli altri giganti della Rete a prendere pubblicamente le distanze dal sistema di sorveglianza globale della Nsa. Tanto più che questa non si accontentava delle informazioni raccolte tramite il programma Prism, ma intercettava all'insaputa delle società interessate le informazioni scambiate dai loro data center sparsi per il mondo.

Nonostante alcuni provvedimenti cosmetici adottati dall'amministrazione Obama, i programmi di sorveglianza globale continuano a operare, compreso Prism. E i giganti del Web si sono adattati. Al punto che continuano a offrire i propri servizi al Pentagono e all'intelligence. Anzi, uno dei boss della Silicon Valley, Pierre Omidyar, che controlla eBay e PayPal, ha di fatto preso il controllo dell'archivio di Snowden, quando nel 2013 ha investito 250 milioni di dollari in First Look, società giornalistica diretta da Glenn Greenwald, Laura Poitras e Jeremy Scahill, il team di giornalisti che hanno raccolto la documentazione dell'ex contractor dell'Nsa. Una forma di gestione dei danni da parte di una persona che ha avuto rapporti con In-Q-Tel e persino con Booz Allen Hamilton.

Tramite la controllata Amazon Web Services (Aws), nel 2013 Amazon ha siglato un contratto da 600 milioni di dollari con la Cia per fornire un servizio cloud che è utilizzato dalle 17 agenzie della comunità d'intelligence. E proprio la Aws è favorita per l'assegnazione del gigantesco programma di cloud computing del Pentagono, la Joint Enterprise Defense Infrastructure (Jedi), dal valore di 10 miliardi di dollari.

L'asserita preferenza del Pentagono per Amazon ha provocato il feroce risentimento della concorrenza e per ora il dipartimento della Difesa ha posticipato la decisione in materia. Tra i possibili concorrenti c'è pure Google, attualmente in posizione di debolezza dopo che lo scorso giugno tremila suoi dipendenti hanno scritto all'amministratore delegato, Sundar Pichai, per protestare contro la partecipazione della società al Progetto Maven, un programma di ricerca che usa l'intelligenza artificiale per etichettare automaticamente i veicoli e le persone riprese dai

14. Cfr. J. ASSANGE, *Quando Google ha incontrato Wikileaks*, Roma 2015, Edizioni stampa alternativa.

droni militari. Al grido di «Google non deve impegnarsi nel business della guerra» i firmatari hanno costretto la dirigenza della società a ritirarsi dal progetto. Così ai primi di ottobre un imbarazzato Pichai si è incontrato con i dirigenti dell'ufficio per l'intelligence del Pentagono nel tentativo di ricucire i rapporti. Senza contare che Google è finita nel mirino del Congresso per la sua volontà di rientrare nel mercato cinese, al prezzo di forti concessioni in favore del governo di Pechino sul fronte della sorveglianza degli utenti.

6. Nei prossimi anni l'alleanza, non sempre serena, tra i giganti americani della Rete e l'apparato difensivo e di intelligence della superpotenza sarà messa a dura prova dall'ascesa della Cina. Sul piano commerciale i Gafa sono sfidati dai Bat (Baidu, Alibaba e Tencent), mentre su quello militare gli Stati Uniti sono insidiati dall'assertività cinese nell'Asia-Pacifico. Forse si arriverà a una divisione delle sfere d'influenza nel mondo¹⁵ e quindi pure nella Rete, come pronosticato dall'ex amministratore delegato di Google, Eric Schmidt, secondo il quale entro il 2030, «vi sarà una biforcazione, con un Internet guidato dalla Repubblica Popolare da una parte, e un Internet non cinese guidato dagli Stati Uniti, dall'altra»¹⁶.


15. C. PELANDA, «Il mercato globale verso la frammentazione», *Milano Finanza*, 5/10/18.

16. Citato in L. KOLODNY, «Ex Google CEO Predicts the Internet Will Split in Two – and One Part Will Be Led by China», *Cnbc*, 20/9/2018, goo.gl/aMbPvS

IL DILEMMA DELL'NSA

di George FRIEDMAN

Nata all'alba della guerra fredda sull'onda del trauma di Pearl Harbor, l'agenzia ha avuto un nuovo impulso dopo l'11 settembre. Complici le nuove tecnologie, la guerra al terrorismo si è volta in un pretesto per violare i diritti civili degli americani.

1.  EL GIUGNO 1942 IL GROSSO DELLA FLOTTA giapponese salpò per conquistare l'isola di Midway. Se l'isola fosse caduta in mani giapponesi, Pearl Harbor sarebbe stato a rischio e i sottomarini statunitensi, impossibilitati a rifornirsi di carburante nel porto, sarebbero stati molto meno efficaci. Lo scopo principale dei giapponesi era sorprendere gli americani e trascinarli in una battaglia navale che non potevano vincere.

La flotta giapponese era enorme. Gli Stati Uniti avevano due portaerei intatte, più una gravemente danneggiata. Ma avevano decrittato il codice delle comunicazioni navali giapponesi e pertanto conoscevano molti dettagli del piano d'attacco nemico. Grazie in gran parte a questa circostanza, un pugno di navi statunitensi devastò la flotta nipponica, alterando così in permanenza l'equilibrio di forze nel Pacifico.

Questo, oltre al vantaggio derivante agli alleati dalla decifrazione dei codici tedeschi, insegnò molto agli americani circa l'importanza dello spionaggio nelle comunicazioni. È lecito supporre che la seconda guerra mondiale sarebbe finita in modo molto meno soddisfacente per gli Stati Uniti se questi non avessero decrittato i codici giapponesi e tedeschi. Se in precedenza gli statunitensi si erano quasi sempre attenuti al famoso principio enunciato da Henry Stimson, in base al quale «i gentiluomini non spiano la posta altrui», alla fine del secondo conflitto mondiale erano ossessionati dal carpire e leggere tutte le comunicazioni rilevanti.

La National Security Agency (Nsa) nacque nel dopoguerra dalla fusione di varie organizzazioni con compiti spionistici. Nel 1951, questa pletora di organismi fu riorganizzata nell'Nsa per intercettare e decifrare le comunicazioni di altri governi in giro per il mondo. Specie quelli dell'Unione Sovietica (allora governata da Stalin) e della Cina (al tempo osteggiata dall'America). L'unico limite all'attività

dell'Nsa era costituito dalla natura tecnica delle comunicazioni, ovvero dal loro essere elettroniche e, dunque, intercettabili.

I flussi di comunicazioni elettroniche crebbero notevolmente nel secondo dopoguerra, tuttavia rappresentavano ancora una parte relativamente esigua del totale. Le risorse erano limitate e dato che al tempo la principale minaccia per gli Stati Uniti era costituita da Stati, l'Nsa si concentrò sulle comunicazioni dei e tra i governi. Nel corso dei decenni, tuttavia, il principio operativo dell'Nsa è rimasto invariato; pertanto, all'aumentare delle comunicazioni elettroniche e digitali, il raggio d'azione dell'agenzia si è ampliato.

2. Alla base di tutto c'è Pearl Harbor. Gli Stati Uniti sapevano che i giapponesi avrebbero attaccato, ma non sapevano dove e quando. Il risultato fu un disastro. Tutto il pensiero strategico statunitense durante la guerra fredda fu costruito a partire da quell'evento e dal terrore che i sovietici potessero lanciare un attacco cogliendo l'America di sorpresa. Il timore di un attacco nucleare imprevisto consentì all'Nsa di spingersi fin dove necessario per violare non solo i codici sovietici, ma anche quelli di altri paesi. L'ignoto è per definizione sconosciuto e data la posta in gioco gli Stati Uniti divennero ossessionati dal conoscere quanto più possibile.

Per raccogliere dati inerenti un possibile attacco nucleare, occorre raccogliere anche una gran quantità di dati che non hanno nulla a che fare con l'attacco in sé. La guerra fredda abbracciò dunque un perimetro molto più vasto delle armi atomiche e le informazioni riguardanti ciò che facevano i sovietici – quali governi avevano asservito, chi lavorava per loro – era una questione cruciale. Non si poteva giudicare cosa fosse importante e cosa no se non dopo averlo letto. Pertanto, la necessità di placare i timori per una possibile «Pearl Harbor atomica» spinse l'America a costruire rapidamente un sistema d'intercettazione globale, il quale raccoglieva enormi quantità di informazioni indipendentemente dalla loro attinenza al confronto bipolare.

Tutto era potenzialmente importante e un sistema d'intercettazione orientato a una singola area o questione rischiava di tralasciare elementi vitali. Così l'ambito d'azione si ampliò, la tecnologia avanzò e l'intrusione nelle comunicazioni private ne fu la logica conseguenza. Non era peraltro una dinamica limitata agli Stati Uniti. Unione Sovietica, Cina, Regno Unito, Francia, Israele e India, nonché ogni altro paese con interessi di politica estera, investivano grandi risorse per raccogliere informazioni elettronicamente. Molto di ciò che era intercettato non veniva letto, perché le capacità di raccolta eccedevano di gran lunga quelle di analisi. Tuttavia, veniva ugualmente raccolto. L'intrusione reciproca divenne sempre più ingente, limitata solo dalle inefficienze degli apparati d'intercettazione e dalla validità dei sistemi crittografici.

3. Il timore di una nuova Pearl Harbor andò scemando dopo la fine della guerra fredda, fino all'11 settembre 2001. Per comprendere l'impatto di quegli attentati, occorre richiamare alla mente le nostre paure. Come individui, noi americani fum-

mo scioccati dagli attacchi: non solo per la scala della devastazione e le modalità impensabili, ma anche perché giunsero totalmente imprevisi. Gli attentati terroristici non erano rari, ma questi sollevarono un nuovo interrogativo: cosa ci aspetta ora? Sembrava infatti che al-Qā'ida fosse capace di altre e ancor più terribili azioni. La paura si impossessò della nazione: era un timore giustificato e sebbene fosse condiviso da altri paesi, negli Stati Uniti risultava totalizzante.

In parte le paure scaturivano dal fallimento dell'intelligence nel prevedere gli attentati. La gente non sapeva cosa riservasse il futuro e, quel che è peggio, riteneva che nemmeno i servizi lo sapessero. Fu creata una commissione federale per studiare cosa fosse andato storto negli apparati della difesa. Il presidente fu accusato di aver ignorato gli avvertimenti, ma la Cia (Central Intelligence Agency) ammise di non avere agenti infiltrati in al-Qā'ida. Pertanto, l'unico modo di monitorare l'organizzazione era intercettarne le comunicazioni: era un lavoro per l'Nsa.

Al-Qā'ida era una rete globale. Il suo monitoraggio permise di comprendere che essa si manteneva unita e si coordinava mediante una nuova, vasta rete di comunicazione in cui era facile mimetizzarsi: Internet. In una fase, al-Qā'ida comunicava nascondendo messaggi in immagini spedite per posta elettronica e usando account anonimi di Hotmail. Per scovare le comunicazioni giapponesi si frugava l'etere, per trovare i messaggi di al-Qā'ida occorreva setacciare Internet.

Si trattava però di cercare un ago in un pagliaio: poche centinaia di uomini nella moltitudine dell'umanità, poche decine di messaggi tra centinaia di miliardi. Inoltre, data la natura della Rete, i messaggi non originavano necessariamente dal luogo in cui era situato il mittente e non approdavano necessariamente dove risiedeva il destinatario. La necessità, dunque, di setacciare l'intero pagliaio alla ricerca dell'ago portò a Prism e ad altri programmi dell'Nsa.

L'obiettivo era scongiurare altri attacchi di al-Qā'ida; il mezzo era violare le comunicazioni dell'organizzazione per leggerne piani e ordini. Per trovare questi ultimi era necessario esaminare tutte le comunicazioni globali, in quanto l'anonimato di Internet e la sua natura multicentrica facevano sì che ogni messaggio fosse potenzialmente quello che si stava cercando. Niente poteva essere scartato, tutto era sospetto. Era la realtà, non il frutto di paranoie.

4. Tra le implicazioni di questa realtà vi era il fatto che l'Nsa non potesse escludere dal monitoraggio le comunicazioni di e tra cittadini statunitensi, perché alcuni membri di al-Qā'ida erano appunto cittadini americani. Era certamente una violazione dei diritti civili, ma non la prima: durante la seconda guerra mondiale, gli Stati Uniti imposero la censura postale al personale militare e l'Fbi (Federal Bureau of Investigation) intercettò determinate lettere spedite all'interno del paese e dall'estero. Il governo creò altresì un sistema di censura volontaria dei media che per molti aspetti non era poi così volontario. Più nota la sospensione dei diritti civili dei cittadini di origine giapponese, che si videro confiscare i beni e rinchiusere in appositi campi governativi. I membri delle organizzazioni filo-tedesche furono perseguiti e arrestati anche prima di Pearl Harbor. Decenni prima, Abraham Lincoln

sospese l'*habeas corpus* durante la guerra di secessione, di fatto consentendo l'arresto e l'isolamento di cittadini senza un giusto processo.

Vi sono però due differenze fondamentali tra i suddetti episodi e la guerra al terrorismo. Primo: il secondo conflitto mondiale cominciò con una dichiarazione formale di guerra. Secondo: la costituzione degli Stati Uniti autorizza esplicitamente il presidente a sospendere l'*habeas corpus* in caso di ribellione. La dichiarazione di guerra conferisce al presidente determinati poteri, in quanto comandante in capo, analogamente alla ribellione. Nessuna di queste condizioni era tuttavia presente quando l'Nsa ha intrapreso programmi come Prism.

Inoltre, in parte per il fondamento costituzionale delle azioni e in parte per la natura dei conflitti, la seconda guerra mondiale e la guerra di secessione ebbero una fine definita, un momento nel quale i diritti civili andavano ripristinati o si doveva porre in essere un processo volto al loro ripristino. Nel caso della guerra al terrorismo, un simile esito non esiste. Come osservato in occasione della maratona di Boston del 2013 (e come del resto attestato da innumerevoli episodi occorsi negli ultimi secoli), costruire ordigni improvvisati è così facile da rendere relativamente semplice ed economico eseguire attentati altamente letali. Alcuni complotti possono essere intercettati e sventati monitorando tutte le comunicazioni, ma chiaramente l'attentato alla maratona di Boston era impossibile da prevedere.

Il problema della guerra al terrorismo è che, non potendo alcun presidente dichiararla formalmente chiusa, manca di criteri chiari e oggettivi di successo. Essa non definisce dei livelli di terrorismo tollerabili; ha come scopo l'azzeramento completo del terrorismo, di matrice islamica e non. Ciò ovviamente non avverrà mai, sicché programmi come Prism e simili andranno avanti indefinitamente, in barba alle blande misure adottate nel frattempo dal Congresso per limitarli. Queste intrusioni, a differenza delle precedenti, hanno obiettivi irraggiungibili e pertanto configurano una sospensione permanente dei diritti civili. In assenza di emendamenti costituzionali, dichiarazioni formali di guerra o di uno stato d'emergenza, l'esecutivo abusa del suo potere a danno dei suoi stessi cittadini.

Dalla fine della seconda guerra mondiale, i requisiti costituzionali per fare una guerra si sono progressivamente assottigliati. Truman usò una risoluzione dell'Onu per giustificare la guerra di Corea, Lyndon Johnson giustificò un conflitto su vasta scala con la risoluzione del Golfo del Tonchino, equiparandola a una dichiarazione di guerra. Il caos concettuale della guerra al terrorismo ha escluso qualsiasi tipo di dichiarazione e ha anche incluso arbitrariamente la Corea del Nord nell'«asse del male» contro cui combattevano gli Stati Uniti. L'ex collaboratore dell'Nsa Edward Snowden è accusato di aver aiutato un nemico che non è mai stato legalmente designato tale. Chiunque anche solo contempra il terrorismo è di per sé un nemico. Nel caso di al-Qā'ida il nemico era chiaro, ma essendo questa un soggetto fluido e non una rigida entità nazionale, la definizione di nemico si è da allora allargata ad includere chiunque – anche singoli individui – concepisca e/o attui un numero infinito di azioni. In fin dei conti, come definire il terrorismo e come distinguerlo dal crimine?

5. Gli attentati dell'11 settembre hanno fatto tremila vittime e sappiamo che al-Qā'ida intendeva ucciderne di più, perché lo ha affermato. Quello e altri movimenti jihadisti, ma anche le formazioni terroristiche non affiliate a movimenti islamisti, rappresentano una minaccia. Alcuni dei loro membri sono cittadini americani, altri no. Prevenire simili attacchi, piuttosto che perseguirne i responsabili una volta che siano stati realizzati, è importante. A tal fine programmi come Prism possono risultare necessari, anche se i profani faticano a valutarne appieno l'utilità.

Al contempo, la minaccia che con tali strumenti si combatte va posta in prospettiva. Alcune minacce terroristiche sono pericolose, ma è semplicemente impossibile fermare qualsiasi imbecille voglia far esplodere una bomba artigianale per ragioni politiche. La domanda chiave è dunque se il pericolo posto da una minaccia terroristica sia sufficiente a giustificare lo sprezzo per lo spirito della costituzione. Se lo è, allora si dichiara formalmente guerra o lo stato d'emergenza. Il pericolo insito in Prism e in altri programmi del genere è che la decisione di avviarli non è stata presa a seguito di un chiaro pronunciamento del Congresso e del presidente in merito all'esistenza di una guerra. È allora che la costituzione è stata minata e l'opinione pubblica americana è corresponsabile, perché lo ha permesso.

Prism e consimili non sono frutto di una volontà dispotica di dominio del mondo. In modo molto più chiaro, logico e comprensibile scaturiscono dall'esperienza passata della guerra e dai legittimi timori per rischi reali. L'Nsa è stata incaricata di fermare il terrorismo e ha sviluppato un piano che non era così segreto come molti sostenevano. Chiaramente non aveva l'efficacia che alcuni auspicavano, altrimenti non vi sarebbe stato l'attentato alla maratona di Boston. Se il programma era finalizzato a sopire il dissenso, ha certamente fallito, come dimostrato dai sondaggi e dalla posizione dei media.

Le rivelazioni su Prism non sono certo nuove e interessanti di per sé: l'Nsa fu creata per fare questo genere di cose e data l'evoluzione tecnologica era inevitabile che si arrivasse a un monitoraggio delle comunicazioni su scala globale. Molte rivelazioni precedenti a quelle di Snowden mostrano del resto che si stava andando in questa direzione. La vera notizia sarebbe stata scoprire che l'Nsa non spiava il mondo intero. Ma tutto questo ci dà l'opportunità di valutare quanto accaduto e di decidere se sia tollerabile o meno.

Il problema dei programmi come Prism non è solo e tanto a cosa siano serviti finora, ma cosa potrebbe avvenire se si consente che proseguano. Non si tratta di un dilemma relativo solo agli Stati Uniti, ma certo sarebbe opportuno che il buon esempio partisse dal paese che più di tutti afferma di essere fedele alla propria costituzione e di rispettarne scrupolosamente lo spirito, oltre che la lettera. Non è un sentiero privo di incognite. Come disse Benjamin Franklin, «chi è disposto a barattare la propria libertà per un po' di sicurezza non merita né libertà, né sicurezza».*

(traduzione di Fabrizio Maronta)

* Questo articolo è apparso originariamente su *Stratfor*.



LA RETE A STELLE E STRISCE

Parte II

DOVE *e* **COME**
si **DIFENDONO** *gli* **ALTRI**

GEOPOLITICA DELLA PROTEZIONE

di *Alessandro ARESU*

Gli Stati Uniti si attrezzano per vincere la guerra fredda tecnologica con la Cina. L'Internet delle cose allarga la sfera delle infrastrutture da proteggere: compito dello Stato. Il Cfius e la lotta alla penetrazione cinese nello hardware. L'Ue è out, la Francia no.

*Se avete qualcosa di
davvero importante da dire,
scrivetelo a mano.*

Donald J. Trump

1.  «ROTEZIONE» È UN CONCETTO DI ALTO rilievo geopolitico. Il capitano Mahan lo adopera sovente nei suoi scritti. Con la maiuscola, *Protection* è l'uso strumentale o strategico del protezionismo commerciale. La protezione riguarda anche, nella sua articolazione marittima, l'approccio verso le stazioni navali, ottenute attraverso l'occupazione militare o il consenso della popolazione.

Così come il commercio non ha un'esistenza separata dalle dinamiche geopolitiche, lo stesso accade per la tecnologia, che sarebbe senz'altro oggetto degli scritti di un Mahan contemporaneo. La geopolitica della protezione¹ è la prosecuzione della guerra economica² in un'arena tecnologica più matura. Identifica tre categorie: a) la protezione dei cittadini dalla tecnologia, per orientarne e limitarne lo sviluppo; b) le contrattazioni delle grandi imprese tecnologiche con gli Stati; c) gli strumenti con cui gli Stati, nei loro organismi nazionali o nel contesto internazionale, sviluppano e favoriscono strumenti, normativi e militari, di controllo degli investimenti, in particolare in ambiti ad alta tecnologia.

2. La prima categoria, la protezione dalla tecnologia, pone davanti una questione di sopravvivenza: cosa faremo se la «Provvidenza tecnologica» abolirà la

1. Riprendo qui i ragionamenti sviluppati in A. ARESU, M. NEGRO, *Geopolitica della protezione. Investimenti e sicurezza nazionale: gli Stati Uniti, l'Italia e l'UE*, Fondazione Verso l'Europa, novembre 2018. Il volume sviluppa questi argomenti attraverso l'analisi estesa della normativa relativa al Cfius.

2. Sulla guerra economica, si vedano i saggi raccolti in *Economic Warfare. Storia dell'arma economica*, a cura di V. ILARI e G. DELLA TORRE, Quaderno Sism 2017. Sull'intelligence economica, sempre utile il documento pionieristico di P. SAVONA, «Presupposti, estensione, limiti e componenti dell'organizzazione dell'intelligence economica», *Per aspera ad veritatem*, n. 15, 1999, pp. 1023-1033.

geopolitica? L'interazione tra tecnologia e geopolitica non è nuova. Il primato mondiale degli Stati Uniti si lega allo sviluppo e all'uso strategico di mezzi scientifici e tecnologici. Secondo un preciso obiettivo: la «frontiera infinita» della tecnologia è figlia della frontiera americana. E con una nota implicita: l'infinito deve riguardare Washington, mentre agli altri deve essere precluso. Questo scenario tecnologico si trova in accelerazione. Lo sviluppo cibernetico diffonde ed estende le capacità di attacco³, e quindi si interseca coi conflitti già esistenti. La dimensione spaziale è sempre presente nell'era della Rete, perché «l'accesso e la fruizione dei servizi di Internet passa necessariamente attraverso l'utilizzo e l'installazione di un'infrastruttura fisica che permette la connessione dei diversi apparati»⁴. Tuttavia, l'immaginazione della fantascienza ci aiuta a gettare il cuore oltre l'ostacolo, eliminando il fattore umano. Cosa accadrà quando il pianeta, dopo la classica *robocalypse* (apocalisse robotica), sarà controllato da entità robotiche avanzate? Nel caso in cui l'umanità sopravviva, per esempio in una resistenza volta a colpire le strutture fisiche dei robot padroni, allora la geopolitica continuerà a esistere. Nel caso in cui l'umanità non sopravviva, la geopolitica non ci sarà più. Questa stessa rivista, sopravvissuta per il divertimento dei successori dell'umanità, sarà scritta da diverse voci dell'intelligenza artificiale.

Il dibattito sull'approssimarsi dell'apocalisse indotta dalla tecnologia è vasto. Include futurologi, regolatori, imprenditori e ciarlatani. Spazia da chi sottolinea la nostra distanza da «Terminator» a chi, come il fondatore di SpaceX e Tesla, Elon Musk, ritiene l'intelligenza artificiale la nostra fondamentale minaccia esistenziale. Musk invoca una maggiore regolazione, nazionale e internazionale, per proteggere l'umanità⁵. I programmi degli Stati sulla cibersicurezza sono, in questo senso, elementi di geopolitica della protezione. Il primo pilastro della strategia cibernetica dell'amministrazione Trump è «Protect the American People, the Homeland, and the American Way of Life»⁶. Non è detto, tuttavia, che la protezione non possa applicarsi a opzioni più estreme. Durante i festeggiamenti per il Capodanno 2017, l'allora presidente eletto Trump, interrogato sulla cibersicurezza, suscitò le risate degli specialisti. Semplice e diretto, come sempre, il lessico della sua «dottrina»: nessun computer è sicuro, se avete qualcosa di davvero importante da dire fate alla vecchia maniera, scrivete a mano e trovate un corriere, uno di fiducia. Lo scetticismo di Trump deriva dalle sue preferenze personali, da una dieta tecnologica in cui imperano le telefonate, Twitter e soprattutto la televisione (o le telefonate davanti alla televisione), ma non è previsto l'uso del computer.

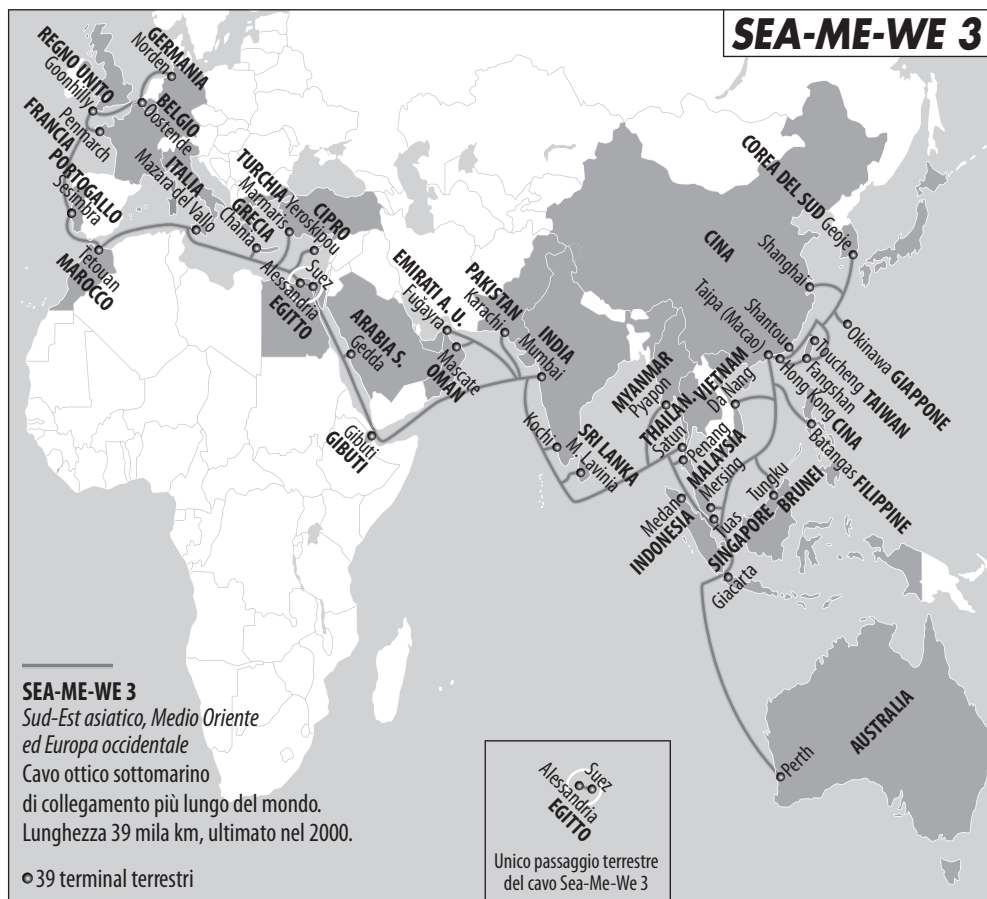
Eppure, le parole di Trump pongono una questione di geopolitica della protezione: la recessione tecnologica. Il passaggio principale della discontinuità tecno-

3. Su questi aspetti, si veda B. WITTES, G. BLUM, *The Future of Violence: Robots and Germs, Hackers and Drones – Confronting a New Age of Threat*, New York 2015, Basic Books.

4. P. CELLINI, *La rivoluzione digitale. Economia di internet dallo Sputnik al machine learning*, Roma 2018, Luiss University Press, p. 144.

5. Le affermazioni di Elon Musk al Mit nel 2014 sono disponibili presso l'accurata sezione «Transcripts» del sito *Shit Elon Says*, goo.gl/5qESMZ

6. *National Cyber Strategy of the United States of America*, settembre 2018.



logica in corso è che l'Internet delle cose rende «critiche» infrastrutture che prima non lo erano. La connettività può riguardare gli elettrodomestici e i mezzi di trasporto, oltre alle infrastrutture dei servizi pubblici e i sistemi di sicurezza privati. Ciò aumenta la vulnerabilità di ogni sistema con cui gli uomini si interfacciano. lato, come vedremo, questo porta ad allargare le maglie della cosiddetta «sicurezza nazionale», fornendo nuove modalità di intervento degli Stati e di esercizio della sovranità. Dall'altro, o crediamo che il processo in corso sia inevitabile, e quindi non crediamo alla libertà umana, oppure possiamo pensare alla riduzione dei rischi. Il crittografo Bruce Schneier, che invece di «Internet delle cose» utilizza l'espressione «Internet+», per sottolineare che ogni cosa è Internet, suggerisce che alla fine della «luna di miele» della computerizzazione e della connettività ci sarà una reazione. La reazione, secondo Schneier, non «sarà guidata dal mercato, ma da norme, leggi e decisioni politiche che mettano la sicurezza e il benessere della società sopra gli interessi delle aziende e delle industrie. Ci sarà bisogno di un forte cambiamento sociale, che per alcuni sarà difficile da digerire, ma la nostra sicu-

rezza dipende da questo»⁷. Le analogie presentate da Schneier, l'energia nucleare e l'avionica, indicano l'importanza di erigere forti standard di regolazione e, se necessario di disconnessione. Agli attori geopolitici resta il loro compito storico: governare la sicurezza, attraverso la violenza della legge e delle armi. È un compito che alcuni possono esercitare, anche l'uno contro l'altro. La lezione di Max Weber sul potere non è superata, bensì approfondita dallo sviluppo tecnologico, che pone con più urgenza la solita domanda di fondo: chi esercita il monopolio della violenza legittima? E chi lo esercita nel numero due e nel numero uno della «frontiera infinita», la Cina e gli Stati Uniti?

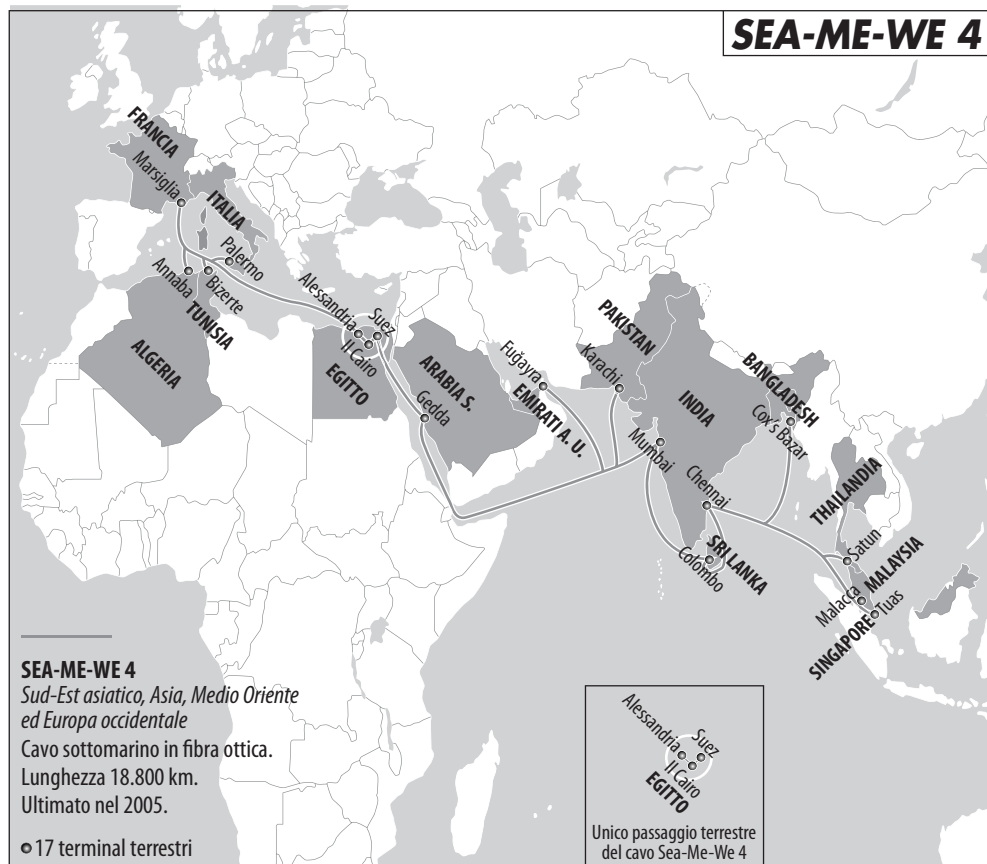
3. L'ascesa cinese degli ultimi quarant'anni può essere raccontata anche come un rilancio scientifico-tecnologico. Inserendo, nel 1978, la scienza e la tecnologia (al fianco di agricoltura, industria e difesa) tra le «Quattro Modernizzazioni», Deng certificò un'azione già portata avanti nella seconda metà degli anni Settanta per migliorare il rapporto tra il Partito comunista cinese e gli scienziati, nonché per avviare relazioni e scambi in materia scientifica e tecnologica con il Giappone e gli Stati Uniti⁸. Nella visione cinese di lungo periodo della storia, il «secolo di umiliazione» della Cina è legato anche al ritardo tecnologico rispetto alle potenze coloniali europee e alla capacità nipponica di utilizzare le capacità occidentali come fattore di potenza. Il ritorno della Cina all'altezza della sua storia e della sua demografia passa per un recupero definitivo di questo ritardo. Il Partito comunista cinese non cela questa consapevolezza. Nello straordinario discorso di Xi Jinping agli scienziati e ingegneri nel 2014⁹, si ripercorrono tutti i fattori della potenza tecnologica cinese: il primato robotico, il suo uso industriale, il «completamento» della modernizzazione con caratteristiche cinesi attraverso la crescita delle pubblicazioni scientifiche, dei brevetti e della forza lavoro impiegata nei centri di ricerca.

Secondo la leadership cinese, non è mai sufficiente fornire un elenco di risultati e di tecnologie chiave. Bisogna partire dalla profondità storica. Xi riprende il grande problema della civiltà cinese: il momento in cui la scienza e la tecnologia dell'Impero del Centro, tra la fine della dinastia Ming e l'inizio della dinastia Qing, sono rimasti drammaticamente indietro. Xi ricorda l'interesse dell'imperatore Kangxi per la scienza e le tecnologie occidentali e ne trae due lezioni. La prima è la scarsa visibilità e diffusione nella società di questi interessi, rappresentati dalla reclusione del grande atlante fatto realizzare da Kangxi. Bisogna combattere la tendenza a tenere la scienza come un segreto o un hobby, perché ciò indebolisce il suo uso come fattore di potenza. «Le conoscenze, per quanto ricche, non pos-

7. B. SCHNEIER, *Click here to Kill Everybody*, capitolo «What a Secure Internet+ Looks Like», New York-London 2018, W.W. Norton & Company.

8. Per gli obiettivi di Deng Xiaoping in materia, si veda E. VOGEL, *Deng Xiaoping and the Transformation of China*, Cambridge MA 2011, Harvard University Press.

9. XI JINPING, «Accelerare la transizione da un modello di sviluppo basato su fattori produttivi e investimenti a un modello basato sull'innovazione», 9/6/2014, in Id., *Governare la Cina*, Firenze 2016, Giunti Editore, pp. 147-161. Estratti del discorso sono disponibili anche nel sito dell'Associazione Stalin, nella sezione «La Cina oggi: ben scavato vecchia talpa?», goo.gl/X17yBh



sono influenzare la società reale se sono archiviate come curiosità, interessi raffinati, o addirittura come abilità peculiari»¹⁰. Le «truppe degli scienziati e dei tecnici»¹¹ cinesi debbono sentirsi parte di un tutto armonioso. Un sistema aperto, nel senso di tessuto dal Partito e da esso collocato nelle vene della società cinese. La seconda lezione riguarda l'affidamento delle scoperte e delle innovazioni ai missionari stranieri. A redigere l'atlante di Kangxi sono stati i gesuiti francesi, e Xi è lieto di continuare il dialogo con i gesuiti, di ricordare i Matteo Ricci e i Matteo Ripa, di intensificare il dialogo industriale con le altre nazioni, anche attraverso l'acquisizione di aziende strategiche. Ma l'Impero del Centro deve essere più ambizioso. Deve imparare a fare da solo, perché la logica della scoperta e la logica della sicurezza sono intessute: «Solo padroneggiando pienamente le tecnologie chiave è possibile impadronirsi del potere d'iniziativa nella concorrenza e nello sviluppo e garantire la sicurezza economica nazionale, la sicurezza della difesa nazionale e la sicurezza in altri ambiti. Non è sempre possibile fregiare il proprio futuro con i traguardi del passato altrui, né far sempre affidamento sugli altrui

10. *Ivi*, p. 155.

11. *Ivi*, p. 159.

traguardi per elevare il proprio livello tecnico-scientifico; ancor meno possibile fare da appendice tecnologica di altri Stati. Non possiamo essere sempre un passo indietro agli altri, imitandoli pedissequamente. Non abbiamo altra scelta: dobbiamo perseguire l'innovazione autonoma»¹².

Questo concetto di innovazione, non sottoposto a regole, leggi o influenze altrui, regge l'estensione del dominio della sicurezza, sotto la guida del Partito e sotto il principio di *junmin ronghe*, la fusione tra militare e civile. In Cina «i settori dello shipping e delle telecomunicazioni hanno compiuto sviluppi continui nella ricerca, nello sviluppo e nella produzione, attraverso il loro inserimento nell'economia internazionale. Queste capacità tecnologiche sono state convertite in nuove capacità militari»¹³. Il tredicesimo piano quinquennale, con il programma Made in China 2025 e gli investimenti in intelligenza artificiale, rientrano nella logica esposta dal presidente cinese. Le grandi imprese digitali cinesi, come Alibaba, Huawei, Baidu, Tencent, Zte, Ztt, Ftt, non possono muoversi senza l'ombrello del Partito e del suo pensiero strategico. Illustrano l'inconsistenza dell'illusione occidentale di una classe media cinese in contrasto col Partito. Se Jack Ma vuole produrre semiconduttori¹⁴, è incoraggiato a farlo. Se Jack Ma vuole andare in spiaggia a godersi la vita, può farlo. Se Jack Ma vuole agire contro gli obiettivi del Partito, non può farlo.

L'investimento cinese in infrastrutture è volto a portare all'estero capitali e a costituire un presidio fisico – in alcuni casi, anche con potenzialità militari, come per esempio nei porti o della realizzazione di basi – della potenza cinese. L'investimento in infrastrutture non si limita alle autostrade, alle ferrovie, ai porti e agli aeroporti, ma può riguardare anche le reti elettriche, le reti di telecomunicazioni e tutte le infrastrutture relative alla trasformazione digitale. Con «Industria 4.0» e con la realizzazione di catene del valore digitali, le stesse strutture industriali sono parte integrante di una più vasta infrastruttura. Parafrasando Schneier, una Internet+ con caratteristiche cinesi, che mette a frutto a livello domestico la grande disponibilità di dati posseduti dal Partito, e a livello internazionale i punti di accesso delle infrastrutture su cui la Cina si estende. Punti di accesso per obiettivi geopolitici: come gli Stati Uniti hanno utilizzato la politica della porta aperta (*open door policy*) nel commercio all'epoca di Mahan, oggi i cinesi sono accusati di utilizzare la politica della *backdoor* (*backdoor policy*), per superare le difese dei dispositivi e dei sistemi informatici, anche attraverso la componentistica hardware¹⁵.

Dati e luoghi costituiscono insieme la collana di perle delle «vie della seta digitali». Pensiamo al progetto Peace (*Pakistan & East Africa Connecting Europe*), il

12. *Ivi*, pp. 151-152.

13. A. SEGAL, *Chinese Technology Development and Acquisition Strategy and the U.S Response*, dichiarazione allo House Committee on Financial Services, Monetary Policy and Trade Subcommittee, 12/12/2017, goo.gl/zAKwvv

14. A. MINTER, «Why Can't China Make Semiconductors?», *Bloomberg*, 30/4/2018, goo.gl/QB7Y1b

15. Questa è l'accusa riportata tra l'altro da un'inchiesta di *Bloomberg* e respinta dalle imprese americane, in J. ROBERTSON, M. RILEY, «The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies», *Bloomberg*, 4/10/2018, goo.gl/JoDKGm

sistema di 12 mila chilometri di cavi con cui Hengtong e Huawei puntano a unire l'Asia, l'Africa e l'Europa. Come ricordano gli storici, «i cavi sottomarini che hanno connesso i continenti, cancellando le distanze oceaniche, furono il genere di miracoli moderni che hanno ispirato la fantascienza di Verne»¹⁶. Tuttavia, gli oceani non sono stati «annullati» dalla connessione dei cavi sottomarini. Al contrario, la loro connessione ha accentuato il rilievo del controllo degli oceani sul piano militare. La vulnerabilità dei cavi e la loro riparazione sono infatti all'attenzione della Marina militare statunitense, come il pericolo che altre potenze, a partire da Cina e Russia, possano attentare alla sicurezza dei cavi, in cui passa circa il 97% delle comunicazioni globali¹⁷. Per esempio, in uno scenario di conflitto su Taiwan, si può immaginare una strategia mirata di Pechino per escludere l'isola dalle comunicazioni, tagliando i cavi sottomarini.

Tutte le questioni sopra descritte non generano l'abrogazione della geopolitica da parte della tecnologia, ma una dinamica di conflitto e negoziazione. Il suo effetto è l'allargamento dei concetti di «sicurezza nazionale» e «infrastrutture critiche» per le potenze che possono permetterselo. Su questa base possiamo leggere i rapporti geopolitici con le grandi imprese digitali, creature ambigue, che non vanno né esaltate con presunzioni di onnipotenza («Nick Clegg dirige gli affari internazionali di Facebook, quindi è l'uomo più potente del mondo!») né ridotte a radice dei mali del mondo. Più utile coglierne il segno geopolitico e i rapporti coi governi.

Prendiamo Amazon, una creatura ormai matura, entità di grande interesse, sul cui destino negli Stati Uniti si è sviluppato un nuovo dibattito antitrust, soprattutto grazie ai lavori di Lina Khan. Al contrario della Compagnia delle Indie Orientali, Amazon non possiede un esercito propriamente detto. Dispone tuttavia di un esercito di utenti, più vasto di qualunque forza militare, e può creare un esercito di lobbisti. Per operare, nell'e-commerce come nel *cloud*, ha bisogno di spazi, di luoghi. Per parafrasare il complesso industriale-militare di Eisenhower, Amazon è un complesso tecnologico-logistico. La sua nuvola ha una struttura fisica e deve radicarsi nei luoghi per alimentarsi. Se vuole inserire lo spazio nella sua Rete (ed è una grande passione di Bezos con Blue Origin), ha bisogno di ottenerne l'accesso da parte del governo americano, altrimenti nello spazio non ci può andare. L'estensione del potere di Amazon richiede una contrattazione continua con gli apparati degli Stati Uniti. Le spese di lobbying sono aumentate del 400% dal 2012 a oggi¹⁸.

Cruciali sono i rapporti tra i servizi di *cloud* di Amazon e il governo della difesa e della sicurezza. Sean Roche, vicedirettore dell'innovazione digitale della

16. S.C. TOPIK, A. WELLS, «Commodity Chains in a Global Economy», in *A World Connecting (1870-1945)*, a cura di E. ROSENBERG, Cambridge Ma 2012, The Belknap Press of Harvard University Press, p. 664.

17. È un tema affrontato in R. SUNAK, *Undersea Cables. Indispensable, Insecure*, Policy Exchange, 2017, goo.gl/tAOZJE

18. S. SOPER, N. NIX, B. ALLISON, «Amazon's Jeff Bezos Can't Beat Washington, so He's Joining It: The Influence Game», *Bloomberg*, 14/2/2018, goo.gl/MSSBGc

Cia, ha lodato la collaborazione tra Amazon e l'agenzia, cementata da un contratto del 2013. La prima slide della sua entusiastica presentazione al summit organizzato nel giugno 2018 a Washington da Amazon è un ringraziamento a Amazon Web Services¹⁹. Jeff Bezos in persona è intervenuto per difendere il coinvolgimento di Amazon con il Pentagono, e in particolare con il contratto Jedi (Joint Enterprise Defense Infrastructure) da 10 miliardi di dollari per il *cloud* del dipartimento della Difesa²⁰. Nel 2016, Bezos ha attaccato Peter Thiel per il suo sostegno a Trump, ma Amazon Web Services fornisce servizi per Palantir, l'azienda cofondata da Thiel che supporta l'agenzia Ice (Immigration and Customs Enforcement) per l'attuazione delle politiche di controllo dell'immigrazione dell'amministrazione Trump²¹.

4. Se esiste una guerra fredda tecnologica, una delle creature «abissali» degli apparati americani ne è un campo di battaglia. Si tratta del Cfius, acronimo che identifica il Committee on Foreign Investments in the United States, il comitato interdipartimentale del governo federale che vigila e controlla gli investimenti esteri diretti. Il Cfius è presieduto dal segretario al Tesoro e la sua attività amministrativa è gestita dal direttore dell'Ufficio della sicurezza degli investimenti del dipartimento del Tesoro.

La guerra fredda tecnologica implica un coinvolgimento sempre più marcato dei sottoapparati di sicurezza all'interno dei vari dipartimenti. Le figure che hanno una responsabilità diretta nelle operazioni del Cfius sono, come in ogni apparato, poco note e importanti. Da maggio 2018, a reggere le fila dell'apparato Cfius è Thomas Feddo, avvocato di Alston & Bird con forti credenziali nella sicurezza: laureato all'Accademia navale, tenente nei sottomarini nucleari e per sette anni in forza all'Ofac, l'agenzia che si occupa delle sanzioni economiche degli Stati Uniti. Un altro burocrate di primo piano è Brian Reissaus, già in forza durante l'amministrazione Obama e proveniente dal controllo delle politiche industriali del Defense Security Service²².

Il Cfius è un soggetto di «geo-diritto»²³. Nella sua storia si uniscono, fino a confondersi, considerazioni giuridiche e letture geopolitiche. La sua creazione risale a più di quarant'anni fa. È stato introdotto nell'amministrazione Ford tramite l'ordine esecutivo 11858 nel 1975, come risposta istituzionale ai risultati del Foreign Investment Study Act of 1974²⁴, volto a studiare l'impatto degli investimenti esteri diretti negli Stati Uniti sulla sicurezza nazionale. La sua origine si inserisce nel di-

19. Il video è disponibile all'indirizzo www.youtube.com/watch?v=czc_r7Xzvwc

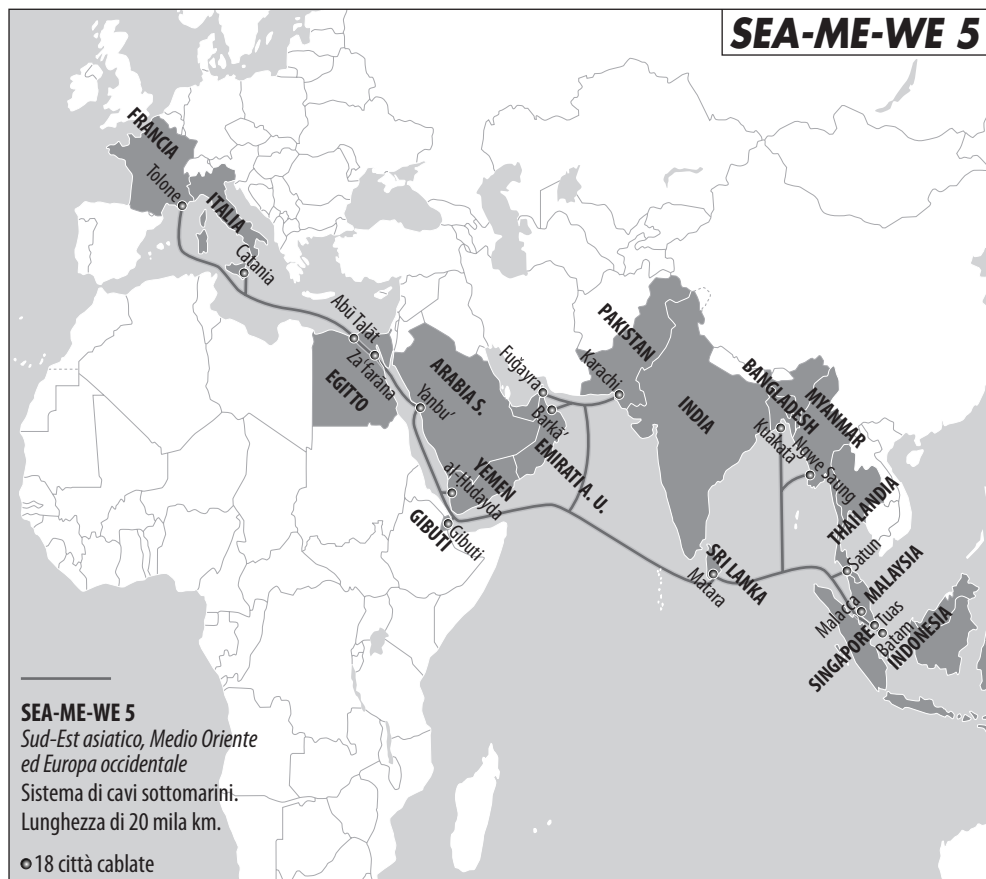
20. H. KELLY, «Jeff Bezos: Amazon Will Keep Working with the DoD», *CNN Business*, 16/10/2018, goo.gl/tVMGkZ

21. Così la lettera di un dipendente di Amazon, «I'm an Amazon Employee. My Company Shouldn't Sell Facial Recognition Tech to Police», *Medium*, 16/10/2018, goo.gl/sGq2RT. Su Thiel rimando a A. ARESU, «L'agenda di Peter Thiel», *Limes*, «L'agenda di Trump», n. 11/2016, pp. 97-103.

22. Si veda B. REISSAUS, «New FOCI Collocation Review Process», in *DSS Access. Official Magazine of the Defense Security Service*, vol. 1, 3, p. 14, goo.gl/Wa8zhr

23. Si veda anzitutto N. IRTI, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari 2001, Laterza.

24. Foreign Investment Study Act of 1974, Public Law No. 93-479, 26/10/1974.



battuto sul «pericolo giapponese», nell'instabilità del sistema alla fine degli accordi di Bretton Woods. Negli anni Ottanta gli investimenti giapponesi negli Stati Uniti destano crescente preoccupazione, ma si dimentica che in termini geopolitici ciò rende il Giappone sempre più dipendente dagli Stati Uniti²⁵.

La Fujitsu nel 1986 si mostra interessata ad acquisire un'azienda storica nello sviluppo americano dei semiconduttori, Fairchild Semiconductor, dove aveva lavorato anche il genio italiano Federico Faggin. L'accordo suscita una forte opposizione nel Congresso e da parte del dipartimento del Commercio, del dipartimento della Difesa (guidato da veterani dall'amministrazione Reagan, Baldrige e Weinberger) e dell'Nsa. Baldrige, campione di rodeo che morirà tragicamente nel 1987 proprio per un rodeo, è duro nelle motivazioni. Indica che l'acquisizione avrebbe creato un effetto domino, erodendo la base tecnologica degli Stati Uniti. Inoltre, un'espansione giapponese nel mercato dei semiconduttori e dell'informatica avrebbe aumentato il deficit commerciale statunitense. Ancor più esplicito l'allora vicesegretario alla Difesa per la sicurezza del commercio Stephen Bryen:

25. G. FRIEDMAN, M. LEBARD, *The Coming War with Japan*, New York 1991, St Martin's Press, p. 149.

«Se una delle nostre aziende di semiconduttori giunge nelle mani dei giapponesi, potremmo finire per non avere più una industria di semiconduttori. Potremmo perdere di default la corsa tecnologica»²⁶. L'impulso congressuale, dovuto soprattutto al senatore democratico del Nebraska John Exon, porta all'approvazione dell'emendamento Exon-Florio al Defence Production Act, istituendo il potere per il presidente di sospendere o proibire fusioni e acquisizioni straniere che mettono in pericolo la sicurezza nazionale, a seguito di un'istruttoria del Cfius. La sicurezza nazionale mantiene una definizione ambigua, nei vari interventi che revisionano il ruolo del Cfius, per esempio nel 2007 con l'approvazione del Foreign Investment in the United States Act (Finsa). Ciò accade perché la sicurezza nazionale, per un impero, è ciò che esso vuole che sia.

Oggi la sicurezza nazionale, nella prospettiva degli Stati Uniti, non è legata solo agli armamenti o alla protezione dal terrorismo, ma riguarda la «capacità tecnologica di lungo termine, il vigore economico e finanziario di lungo termine, e la privacy nel lungo termine dei dati medici e finanziari dei cittadini, oltre che altre forme di dati»²⁷. La sicurezza nazionale non risponde a statiche definizioni politologiche o accademiche. Aderisce alla realtà della propria sopravvivenza. E risponde alle sfide, agli avversari, trasformandosi e adeguandosi. Pertanto, i casi Cfius possono e potranno essere letti anche secondo la lente geopolitica.

La riforma che porta al rafforzamento dei poteri reca il segno di due casi, entrambi emersi del 2005, riguardanti gli investimenti di China National Offshore Oil Corporation e Dubai Ports World. Segni geopolitici dell'importanza della sicurezza energetica e del sistema portuale internazionale.

La situazione presente svela un altro significato dell'acronimo Cfius: Chinese Foreign Investment in the United States. Il principale oggetto di scontro riguarda, ancora una volta, la dimensione spaziale della tecnologia: l'hardware. L'escalation è avviata durante l'amministrazione Obama, con l'offerta d'acquisto di 670 milioni di euro lanciata nel maggio 2016 dal fondo di investimenti cinese Fujian per Aixtron, azienda tedesca focalizzata sui mercati asiatici, quotata alla Borsa di Francoforte e attiva nella produzione di chip. L'operazione è finanziata da Sino Ic Leasing Co, controllata di China Ic Industry Investment Fund, partecipata del governo cinese. Il 2 dicembre 2016 il presidente Obama decide di bloccare la transazione per le attività di Aixtron negli Stati Uniti, poi portando all'abbandono dell'offerta da parte di Fujian. Nel novembre 2016 Canyon Bridge Capital Partners, fondo di *private equity* col sostegno finanziario del governo cinese, annuncia l'intenzione di acquistare Lattice Semiconductor, impresa americana produttrice di semiconduttori, per 1,3 miliardi di dollari. Nel settembre 2017, Trump blocca la transazione²⁸. Nel 2018,

26. B. LOJEK, *History of Semiconductor Engineering*, Berlino-Heidelberg 2007, Springer, p. 173. Stephen Bryen ha ricoperto in seguito diversi altri incarichi in materia di difesa e tecnologia, anche come presidente di Finmeccanica North America e commissario della U.S.-China Security Review Commission.

27. M. KUO, «CFIUS Scrutiny of Chinese Investment. Insights from Robert Hockett», *The Diplomat*, 8/1/2018, [goo.gl/3V2rbd](https://go.gl/3V2rbd)

28. *Order Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited*, 12/9/2017.



i casi Broadcom/Qualcomm e Zte aumentano ulteriormente il rilievo della sicurezza nazionale negli investimenti. Il 12 marzo, Trump blocca l'acquisizione da 117 miliardi di dollari da parte di Broadcom, che ha sede a Singapore, della statunitense Qualcomm²⁹, basandosi sull'istruttoria Cfius. In una lettera del 5 marzo ad Aimen Mir, allora vice sottosegretario al Tesoro per la sicurezza degli investimenti, Trump illustra quanto la decisione sia stata influenzata dalla minaccia cinese. Aggiungendosi alle «ben note preoccupazioni di sicurezza nazionale su Huawei e altre aziende cinesi di telecomunicazioni», l'operazione colpirebbe la capacità di ricerca e sviluppo degli Stati Uniti e, soprattutto, favorirebbe il dominio cinese negli standard 5G, anch'essi di interesse nazionale per gli Stati Uniti³⁰.

29. Presidential Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited, 12/3/2018.

30. La lettera si può consultare nel sito della Sec, goo.gl/JUpQDL

A proposito delle note preoccupazioni: una delle principali imprese digitali cinesi, Zte, nel 2016 è stata accusata di violare le leggi americane sulle sanzioni all'Iran e alla Corea del Nord. Viene raggiunto un accordo monetario nel 2017 tra l'azienda e le autorità statunitensi, che impone alla società una multa e alcune precise prescrizioni. Nell'aprile 2018 il dipartimento del Commercio indica il mancato rispetto da parte di Zte delle prescrizioni e decide di colpirla la giugulare, vietandole per sette anni di acquistare prodotti da fornitori degli Stati Uniti (come i semiconduttori di Qualcomm e Intel). Una mossa in grado di portare Zte alla bancarotta, che infatti nel maggio 2018 annuncia di cessare le proprie operazioni. A seguito di un intervento personale del presidente Trump su richiesta di Xi Jinping, le condizioni imposte a Zte vengono ridotte nel giugno 2018, rendendo possibile la sua sopravvivenza. Previo commissariamento. Il 24 agosto 2018³¹ l'ufficio relativo a industria e sicurezza del dipartimento del Commercio sceglie Roscoe C. Howard, Jr. per coordinare la *compliance* dell'azienda, con un accesso senza precedenti e un mandato molto ampio per monitorare il rispetto delle leggi degli Stati Uniti sul controllo delle esportazioni da parte di tutto il gruppo. L'amministrazione Trump e il Congresso marciano uniti nell'attenzione per il Cfius, espandendo le sue caratteristiche e la sua potenzialità di intervento, tramite il Firmma (Foreign Investment Risk Review Modernization Act). Il 10 ottobre 2018 il dipartimento del Tesoro identifica, *ad interim*, 27 industrie di applicazione, che comprendono la manifattura aeronautica, le batterie, le trasmissioni radiotelevisive e le reti di telecomunicazione, la ricerca e sviluppo in biotecnologie e nanotecnologie. E ovviamente i semiconduttori.

Oggi solo il 16% dei semiconduttori usati in Cina sono prodotti nell'Impero del Centro. È un obiettivo indiretto della sicurezza nazionale degli Stati Uniti impedire alla Cina di raggiungere gli obiettivi di autonomia fissati dalla pianificazione del Partito (40% nel 2020 e 70% nel 2025³²). Per questo Washington potrebbe colpire – se necessario – anche gli altri investitori asiatici che marciano insieme ai capitali cinesi, come la finanza sovrana di Singapore³³.

La guerra fredda tecnologica tra Pechino e Washington può portare sia a ricomposizioni negoziali su altri tavoli che a dissidi ancora più profondi in ambito culturale, fino a barriere reciproche nella ricerca e a una netta riduzione dell'interscambio tra studenti. In questa «trappola di Tucidide tecnologica», altri animali possono restare impigliati. Anzitutto, l'Unione Europea, che si presenta in una posizione di debolezza in merito alla frontiera scientifico-tecnologica rispetto agli Stati Uniti e alla Cina. La capacità di incidere sulla frontiera scientifico-tecnologica richiede, se non il *junmin ronghe* cinese, un circolo virtuoso tra in-

31. Si veda «U.S. Department of Commerce Announces Selection of ZTE Special Compliance Coordinator», Office of Public Affairs, Department of Commerce, 24/8/2018, goo.gl/aPGuX7

32. G. LEVESQUE, «Here's How China Is Achieving Global Semiconductor Dominance», *The National Interest*, 25/6/2018.

33. Il fondo Temasek Holdings è tra gli investitori di Hou An Innovation Fund. Si veda M. CHAN, C. TING-FANG, «Arm's China Joint Venture Ensures Access to Vital Technology», *Nikkei*, 3/5/2018, goo.gl/4ySd6v

dustrie civili e militari, un sentire comune capace di far circolare le idee. Gli Stati dell'Unione Europea dovrebbero uscire dalla loro «vacanza dalla storia» e accettare di vivere in un mondo in cui difesa e sicurezza determinano in modo decisivo l'esistenza e la sostenibilità dei progetti politici. Improbabile. L'Unione Europea sarà oggetto, non soggetto, della geopolitica della protezione. Se non per la sua competizione interna, come quella tra Italia e Francia. Caduto il suo appello per costruire una «Darpa europea», cioè per rafforzare la tecnologia francese coi soldi degli altri, Emmanuel Macron si fa la Darpa francese, sfruttando il proprio lungimirante aumento delle spese militari³⁴. Non nasceranno giganti tecnologici europei che abbiano autonomia militare, e pertanto decisionale. Le regolazioni europee, e i poteri speciali dei vari Stati, andranno perciò considerati come pedine della guerra fredda tecnologica tra Washington e Pechino. Che toccherà la geopolitica della protezione degli algoritmi e dagli algoritmi, ma anche dell'hardware, della logistica, dei cavi.

5. Lo storico israeliano Yuval Noah Harari, che ha venduto dodici milioni di libri, illustra il futuro che ci attende nel 2048. Tra trent'anni, al risveglio mattutino fronteggeremo «migrazioni nello spazio cibernetico, identità di genere fluide e nuove esperienze sensoriali generate da computer impiantati nel corpo». Harari ne è certo: al compimento dei trentacinque anni diremo di essere «una persona di genere indefinito che si sta sottoponendo a un intervento di aggiornamento anagrafico, la cui attività neocorticale ha luogo principalmente nel mondo virtuale New Cosmos, e la cui missione esistenziale è andare dove nessuno stilista è mai andato prima»³⁵. Il novello Marx-Engels non ha dubbi: «Entro il 2048, anche le strutture fisiche e cognitive si dissolveranno nell'aria o in una nuvola di dati»³⁶. O forse anche le sue nuvole, nel 2048, risiederanno più prosaicamente nel presidio geopolitico delle terre e dei mari. Specialmente in terra d'Israele.

34. M.G. BARONE, «Una DARPA francese», *RID*, 3/4/2018, goo.gl/SrEZjx

35. Y.N. HARARI, *21 lezioni per il XXI secolo*, Milano 2018, Bompiani, p. 383.

36. *Ivi*, p. 382.

IL MERCATO UNICO SERVE MA NON BASTA

di Giovanni COLLOT

Internet si divide in blocchi regionali, ma l'Europa gioca in difesa. Multe ai Gafa, regole sulla privacy e digital tax denotano un approccio solo normativo. La sovranità digitale richiede campioni globali capaci di competere con Usa e Cina.

L'

1. UNIONE EUROPEA VA ALLA GUERRA digitale? Questa domanda si ripresenta con regolarità nelle menti e nelle parole di chi segue gli affari europei. Negli ultimi anni, seguendo lo *Zeitgeist* che vede l'economia digitale come il futuro, anche la Commissione, sempre attenta ai fattori di crescita e sviluppo, ha deciso di applicarsi alla materia: il Mercato unico digitale, come viene chiamata la strategia complessiva adottata dall'Ue nel 2015 per rendere il mercato europeo più competitivo nelle nuove tecnologie, è diventato l'argomento principale in molti circoli di Bruxelles.

L'obiettivo del Mercato unico digitale sarebbe «aprire opportunità digitali per i cittadini e le aziende europee e sviluppare la posizione dell'Europa come un leader mondiale nell'economia digitale»¹. Tuttavia, l'iniziativa della Commissione giunge in una fase che vede il mondo digitale sempre più diviso tra le sfere d'influenza americana e cinese².

Alcune iniziative nel panorama internazionale – le multe a Google e ad Amazon, il nuovo regolamento sulla privacy online e la recente proposta di una tassa sulle multinazionali digitali – sembra indicare che l'Unione Europea voglia ritagliarsi il suo posto tra i due giganti globali. In effetti, le azioni europee condotte dal 2015 a oggi nel mondo digitale sono ispirate da rara coerenza³, soprattutto per la portata dei bersagli: le grandi aziende americane di Internet, conosciute nel gergo europeo come Gafa (Google, Amazon, Facebook e Apple). Tanto da spingere molti a ipotizzare che esista una strategia precisa per contrastare il predominio statunitense del mercato digitale. Ricostruzione negata con forza dai vertici della Commissione. Eppure, i dubbi restano.

1. Digital Single Market, Commissione europea, goo.gl/5bTDj7

2. «The Battle for Digital Supremacy», *The Economist*, 15/3/2018.

3. «The Rise of Digital Protectionism», Greenberg Center for Geoeconomic Studies, Council on Foreign Relations, 18/10/2017.

Per verificare l'esistenza di una tale strategia, è utile analizzare il sistema decisionale europeo, partendo da chi comanda. Il tema del controllo di Internet si presta bene a questo esercizio, in quanto i rapporti di forza tendono a evidenziarsi quando la posta in gioco è alta.

2. La strategia europea nel digitale, come tutte le priorità della Commissione, non è limitata a un settore, ma informa tutta l'attività legislativa. La sua pervasività fa sì che sulla scena si muova un numero molto di attori, ognuno con propri interessi, obiettivi e necessità. In questo contesto, le istituzioni europee agiscono come mediatrici di interessi divergenti. Il risultato è un panorama frastagliato di decisioni, dove ogni dossier è affrontato singolarmente.

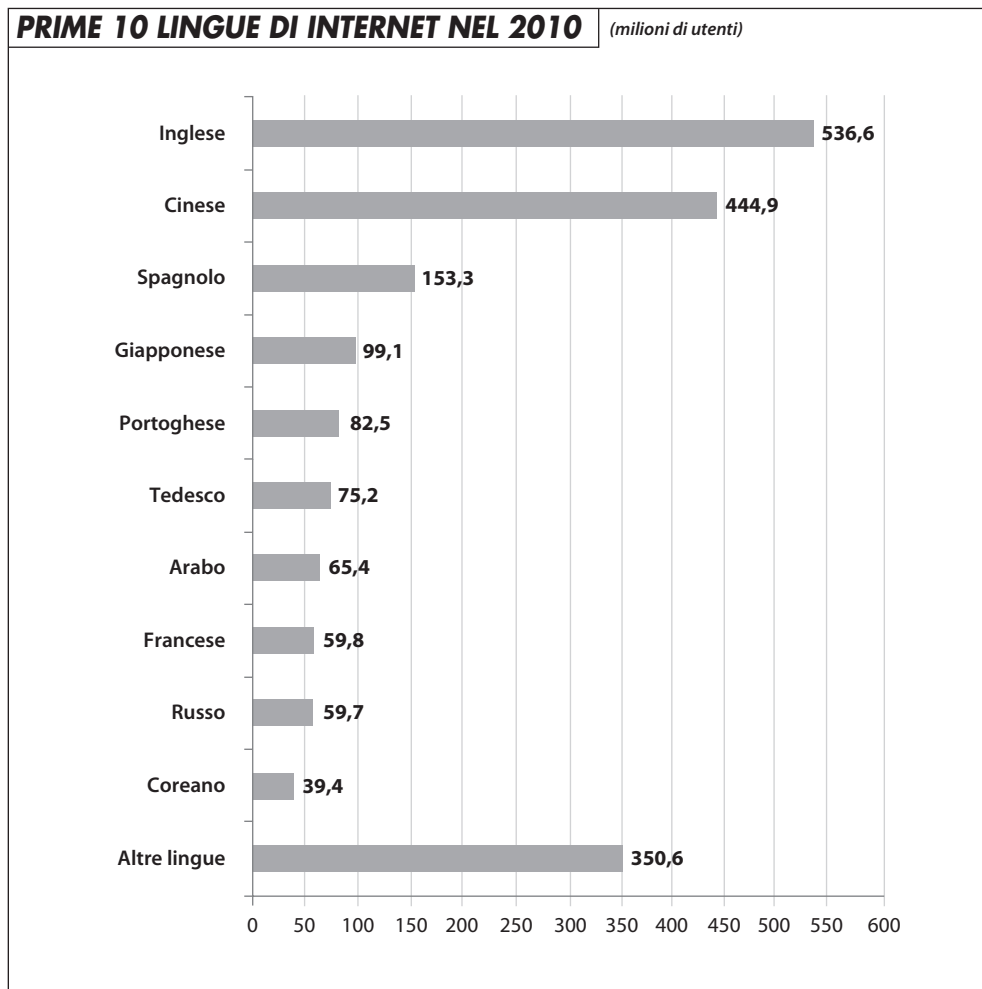
Tre esempi illustrano, in modo diverso, la retorica della guerra contro i giganti della Rete: le inchieste su Google e Amazon della Dg (direzione generale) Concorrenza; la recente direttiva sul diritto d'autore, che ha visto una lotta all'ultimo sangue tra piattaforme e produttori di contenuti; l'attuale dibattito sulla proposta di tassare i redditi delle aziende digitali. Si tratta di tre casi diversi per diffusione dei poteri, protagonisti e processo decisionale; proprio per questo, offrono una visione d'insieme sull'azione dell'Unione.

Il primo episodio riguarda il ruolo della politica sulla concorrenza. Sotto il mandato della danese Margrethe Vestager, commissario alla Concorrenza dal 2014, l'omonima Dg si è presa il centro della scena nella lotta ai Gafa. In nessun altro settore la sua azione è stata più evidente al grande pubblico. Tale centralità è stata ottenuta anche grazie alla capacità politica e comunicativa del commissario e alla rapida successione degli eventi. Per prima cosa, riprendendo un caso risalente al predecessore di Vestager, Joaquín Almunia, la direzione ha inquisito e condannato Google a una multa di 2,42 miliardi di euro per abuso di posizione dominante nei servizi di vendita online⁴. La multa equivale al 6% del giro d'affari del gigante di Mountain View ed è stata salutata da Vestager come una punizione esemplare: «Le aziende dominanti sul mercato come Google hanno una responsabilità particolare nella tutela della libera concorrenza. Abbiamo dovuto multare Google perché ha mostrato di non voler ottemperare alla responsabilità derivante dal suo potere»⁵.

Subito dopo è toccato ad Amazon e ad Apple, condannate per questioni fiscali. Secondo l'accusa, le due aziende avrebbero goduto per anni di imponenti sgravi fiscali da parte dei due paesi in cui hanno la sede europea, rispettivamente Lussemburgo e Irlanda. Se per il gigante dell'e-commerce tali benefici ammontano a 250 milioni di euro, ben più consistente è la cifra non versata da Cupertino: 13 miliardi. Cifre interpretate dalla Commissione europea come indebiti aiuti di Stato. Anche in questo caso, Vestager ha dato al procedimento un significato più ampio: «Spero che le due decisioni siano viste come un messaggio: tutte le società devono

4. L. ROUX, «Google Sentenced: The Struggle between the European Commission and Web Giants», *The New Federalist*, 17/1/2018.

5. M. VESTAGER, «Clearing the Path for Innovation», 7/11/2017, goo.gl/2BLLCW



Fonte: Internet World Stats - www.internetworldstats.com/stats7.htm

pagare il giusto ammontare di tasse e gli Stati membri non possono accordare alle multinazionali benefici fiscali negati alle altre aziende»⁶.

L'approccio della Dg Concorrenza è stato piuttosto lineare: la preparazione di una burocrazia esperta e coesa in una delle direzioni generali più forti della Commissione si è saldata alla guida di un commissario che ha saputo arricchire l'azione amministrativa di una visione politica, sapendola poi comunicare⁷.

Ben diverso l'iter che ha portato alla nuova legge sul diritto d'autore digitale. Dopo che la proposta della Commissione era stata respinta una prima volta dal Parlamento europeo lo scorso luglio, una versione leggermente emendata è stata approvata nella plenaria del 12 settembre. Centrali gli articoli 11 (che introduce

6. R. MONCADA, «The European Union and the GAFA Issue», *Eyes on Europe*, 12/11/2017.

7. T. LARGER, «The Myth of the EU's Apolitical Competition Rule Book», *Politico*, 8/8/2018.

una *link tax*, ovvero la previsione di una retribuzione agli editori da parte dei motori di ricerca che ne condividono gli articoli) e 13, che obbliga le piattaforme (come YouTube o Facebook) a installare software che filtrino i contenuti soggetti a copyright⁸. Dopo un feroce dibattito, il testo approvato premia i produttori di contenuti, cui è riconosciuto il diritto alla retribuzione da parte delle piattaforme. La misura, presentata dal suo principale sostenitore – il parlamentare cristiano-democratico tedesco Axel Voss – come un modo per riequilibrare i guadagni tra produttori e distributori di contenuti, colpisce ancora una volta i giganti digitali.

In questo caso però, trattandosi di un atto legislativo, il processo decisionale ha coinvolto molti più attori, a partire da Günther Oettinger, commissario tedesco a capo del dossier digitale quando la direttiva è stata proposta nel 2016, passando per le varie commissioni del Parlamento europeo e per lo stesso Axel Voss, relatore della proposta. Durante i negoziati sono inoltre intervenute aziende, associazioni di categoria, dirigenti, attivisti e persino celebrità come Paul McCartney, l'inventore di Internet Tim Berners-Lee e il fondatore di Wikipedia Jimmy Wales. Ne è scaturita «la più intensa campagna lobbistica di sempre» a Bruxelles⁹, dai toni a tratti apocalittici: tra timori per la fine «di Internet come lo conosciamo», minacce di cancellare interi siti (da parte di Wikipedia) e solenni promesse di proteggere l'industria creativa europea. Questa, alla fine, l'ha spuntata, anche grazie alla convergenza di interessi tra l'influente industria tedesca dei media e i connazionali Oettinger e Voss.

L'elemento nazionale risulta addirittura preponderante nel terzo caso: l'attuale dibattito sulla proposta della Commissione europea di *digital tax*. La proposta dello scorso marzo prevede d'imporre una tassa europea del 3% sui redditi delle aziende digitali, basata non più sulla loro residenza fiscale, ma su dove sono ubicati i loro utenti. L'idea ruota attorno al concetto di «presenza digitale» e, spiega Matthias Bauer dello European Centre for International Political Economy (Ecipe), «innova profondamente rispetto alle tradizionali modalità del diritto fiscale»¹⁰. Come nel caso dell'ammenda a Google, anche in questo la misura è giustificata con la necessità di costringere le aziende digitali a pagare la loro giusta quota di tasse. Secondo il ministro dell'Economia francese Bruno Le Maire, «proponiamo di fissare un livello di tassazione per assicurarci che questi grandi gruppi paghino quello che devono alle finanze pubbliche dei paesi dove realizzano i loro profitti»¹¹.

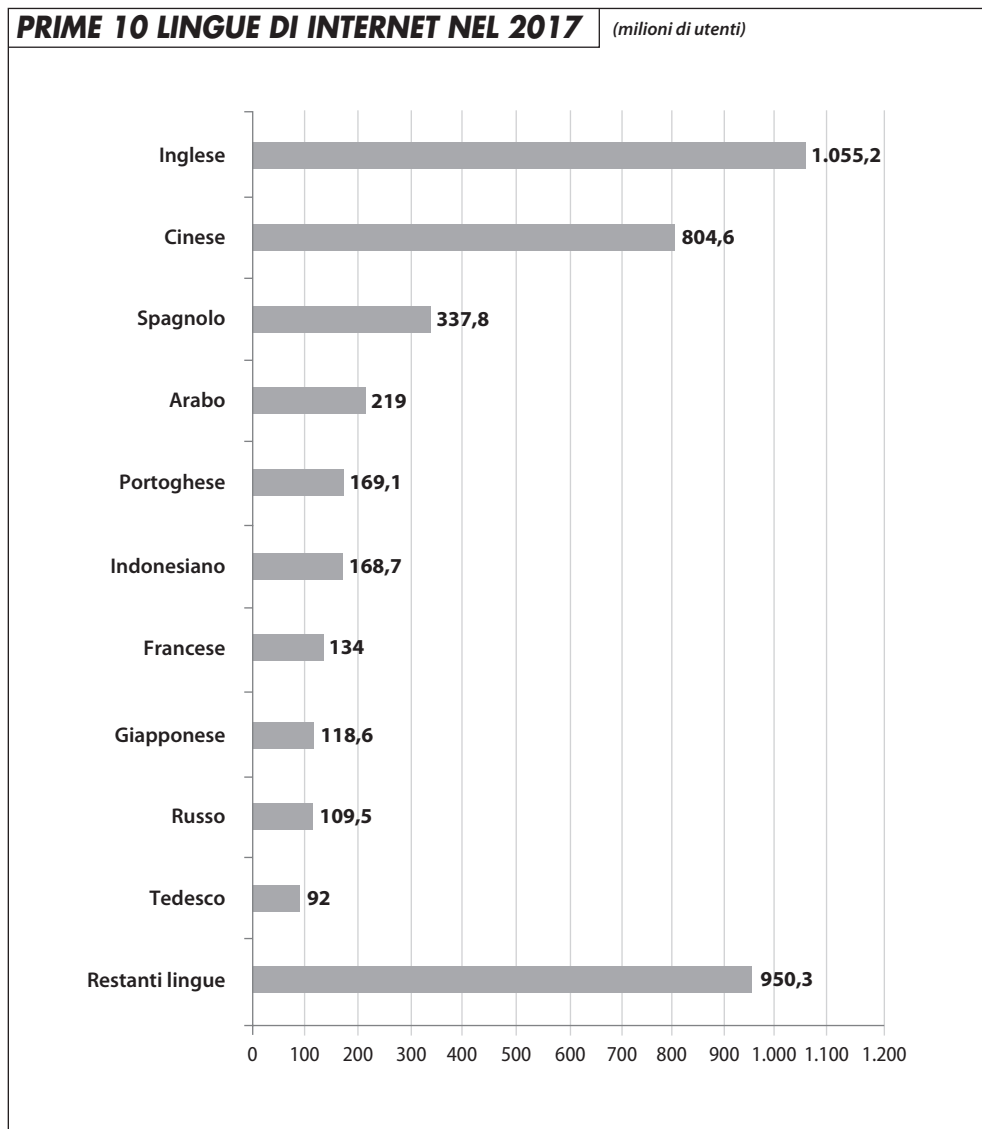
Quella esposta da Le Maire è la linea del governo francese, principale ispiratore della *digital tax*: è Parigi che ha introdotto la prima versione di tassa sul digitale, poi assunta come propria dalla Commissione. Sempre la Francia si è fatta capofila della misura, anche grazie al sostegno decisivo di Pierre Moscovici,

8. J. VINCENT, «EU Approves Controversial Copyright Directive, Including Internet “Link Tax” and “Upload Filter”», *The Verge*, 12/9/2018.

9. «Brussels Gripped by Lobbying War Over Copyright Law», *European Data Hub News*, 4/9/2018.

10. M. BAUER, «Digital Companies and Their Fair Share of Taxes: Myths and Misconceptions», The European Centre for International Political Economy, febbraio 2018.

11. M. DEEN, «Tomek Radoslav e Dendrinou Viktoria, EU Seeks a Digital Tax to Stem the “Bags of Money” Lost to Loopholes», *Bloomberg*, 15/9/2018.



Fonte: Internet World Stats - www.internetworldstats.com/stats7.htm

socialista francese e commissario europeo agli Affari economici, esposti in prima persona per un provvedimento che, nelle intenzioni, dovrebbe anticipare passi analoghi e di più ampia portata da parte dell'Ocse (l'Organizzazione per la cooperazione e lo sviluppo economico).

La politica fiscale resta però appannaggio degli Stati membri. Così, sebbene i 28 si siano detti d'accordo fin da subito nel cercare una soluzione condivisa, sono evidenti le divisioni. Alla Francia, principale sostenitrice di una tassa alta e interessata a proteggere le sue aziende di telecomunicazioni (tra cui Orange, ex France Telecom), si sono allineate l'Austria e, un passo indietro, Italia e Regno

Unito, paesi con consistenti basi di utenti. Sull'altro versante i paesi piccoli – come l'Irlanda, il Lussemburgo o i baltici – il cui modello economico si basa in gran parte sull'attrattività fiscale. In mezzo si situa la Germania: all'inizio grande sostenitrice della legge, negli ultimi mesi si è defilata, per timore di rappresaglie commerciali da parte americana¹². Ciò ha portato Parigi a rilanciare, proponendo all'Irlanda una ricompensa per l'eventuale ammanco di gettito. «Il probabile risultato», spiega Bjarke Smith-Meyer del sito d'informazione *Politico*, «sarà un compromesso. Si arriverà senz'altro a un accordo, perché Parigi e Vienna si sono esposte troppo per rinunciarvi; ma di che natura, si saprà solo all'ultimo»¹³.

3. I tre esempi evidenziano una tendenziale comunanza d'intenti tra istituzioni e Stati membri: riaffermare la sovranità europea contro le grandi aziende globali del digitale. Tra i vari attori che si muovono sulla scena di Bruxelles, sembra maturata negli ultimi anni una certa consapevolezza dell'importanza strategica dello spazio digitale e della conseguente necessità di regolamentarlo. È questo il concetto chiave alla base del Mercato unico digitale.

Eppure è difficile individuare una strategia compiuta per il dominio dello spazio digitale da parte delle istituzioni europee. Piuttosto, a Bruxelles si procede come da prassi, cercando di aggregare un consenso su alcuni valori. Più che sede di un potere verticistico, le istituzioni europee sono una piattaforma per lo scambio di interessi particolari, che sulla questione digitale registrano una fortunata convergenza. Il risultato è una strategia diffusa, non calata dall'alto, ma forse proprio per questo assai pervasiva.

Si tratta però di una strategia strabica, o comunque incompiuta, che espone i limiti della proiezione europea. Infatti, a un'idea definita di mercato interno digitale e agli strumenti per realizzarlo non sembrano ancora corrispondere mezzi altrettanto forti per imporre l'Europa come vera alternativa a Cina e Stati Uniti. L'offensiva contro le aziende americane ha un significato più interno che esterno: le iniziative sui temi del monopolio commerciale, delle tasse e della privacy offrono a politici nazionali e istituzioni europee l'occasione di guadagnare crediti presso i loro cittadini. Le dichiarazioni di Vestager, di Le Maire e dello stesso Macron – secondo cui «gli attori dominanti, soprattutto anglosassoni, non rispettano le regole»¹⁴ – sono figlie di una strategia comunicativa che mira a costruire uno spazio commerciale e industriale comune.

Queste iniziative hanno per lo più un'efficacia geopolitica limitata: proprio perché basate su una comunanza di interessi forte ma temporanea, basta poco a pregiudicarle. Come nel caso della *digital tax*: di fronte alla possibile ritorsione statunitense, l'entusiasmo della Germania – sempre attenta a proteggere la propria catena del valore – è subito venuto meno. Ciò malgrado le ammonizioni

12. J. PLUCINSKA, «Vinocur Nicolas e Smith-Meyer Bjarke, Europe's Digital Tax Map: Where Countries Stand», *Politico*, 6/4/2018.

13. Intervista con l'autore realizzata il 12 ottobre a Bruxelles.

14. M. KHAN, J. BRUNSDEN, «Macron Slams "Anglo-Saxon Tech Giants" for Distorting Competition», *Financial Times*, 29/9/2017.

di Le Maire: «Di cosa abbiamo paura? Degli Stati Uniti? Dovrebbe essere ormai chiaro che Trump rispetta solamente chi è forte e risoluto!»¹⁵. Ma la principale carenza sta nell'assenza di qualsiasi riferimento alla Cina: l'Ue e i suoi Stati membri non hanno semplicemente i mezzi, forse nemmeno l'interesse, a scendere in guerra contro Pechino sul digitale.

Questo non significa che le armi dell'Unione siano completamente spuntate. Tuttavia, l'unica area in cui l'azione europea risulta di una certa efficacia è quella regolamentare: stabilire cioè i criteri d'accesso al mercato unico. Qui l'Ue sembra aver ormai preso piena coscienza della propria forza: le regole sulla concorrenza, sul diritto d'autore e soprattutto sulla privacy mirano, nelle intenzioni, a creare uno spazio di tutela per i diritti dei cittadini europei senza eguali al mondo, secondo il mantra dell'«Europa che protegge»¹⁶. Con effetti, magari preterintenzionali, anche oltre i confini dell'Unione, perché la rilevanza del mercato unico fa sì che gli standard europei condizionino paesi e soggetti terzi che con l'Ue interagiscono. Il discorso, nel caso specifico, attiene soprattutto al forziere dei dati personali, di cui i Gafa sono oggi i grandi depositari.

Nonostante le ambizioni, però, l'Europa rischia di fermarsi a metà del guado sul digitale: un ambito in cui per ora sembra giocare di sponda, accettando l'egemonia statunitense e cercando al massimo di regolarne gli eccessi. Malgrado gli sforzi e le dichiarazioni, l'Ue non appare ancora capace di sviluppare un equivalente di Google o Facebook: delle 200 principali aziende digitali al mondo, solo 8 sono europee¹⁷.

Questo ritardo rischia di diventare una debolezza: in un ecosistema globale che va verso un'Internet divisa per blocchi regionali, è ancora presto per dire se all'Ue basterà essere un mercato appetibile a due egemonie in lotta, o se dovrà invece fare di più per dar vita a una compiuta sovranità digitale¹⁸.

15. «Le Maire Calls for German Backing on Digital Tax, Euro Zone Budget», *Reuters*, 3/19/2018.

16. M. LEONARD, «L'Europe qui protège: penser l'Union européenne à venir», *European Council on Foreign Relations*, agosto 2017.


17. «Europe's History Explains Why It Will Never Produce a Google», *The Economist*, 13-19/10/2018.

18. J. HACKENBROICH, «Reality Bytes: Europe's Bid for Digital Sovereignty», *European Council on Foreign Relations*, 17/10/2018.

RUSSIA E CINA CI HANNO SCIPPATO INTERNET

di James LEWIS

Un punto di vista americano su come le tecnologie informatiche riscrivono la competizione fra grandi potenze. La disillusione verso i miti del progresso lineare. I rivali dell'America le rivolgono contro i suoi stessi mezzi d'influenza. Ma non tutto è perduto.

1.  A TECNOLOGIA INFORMATICA HA rimodellato il conflitto internazionale. La visione degli anni Novanta secondo cui la fine della guerra fredda aveva coinciso con il trionfo della democrazia di mercato si è dimostrata illusoria. Diverse forti tendenze – compresa la reazione alla supremazia degli Stati Uniti, il decadimento dell'ordine internazionale creato dopo il 1945 e l'effetto politico delle tecnologie dell'informazione – stanno riscrivendo la sicurezza globale. La competizione strategica si gioca non sul *jihād* e nemmeno sulla difesa di immaginari beni comuni mondiali, ma su come il mondo sarà ordinato e su chi sarà a farlo.

La reazione al globalismo e alla diffusione della cultura occidentale e americanizzata ha fatto tornare in auge il nazionalismo, con le varie società che cercano di proteggere i propri valori. Il tutto accompagnato da un generale scontento nei confronti dei valori occidentali e dei diritti individuali che un tempo si pensava incarnassero il progresso. È l'antitesi dell'approccio da «mondo senza confini» dei visionari di Internet. Ad acuire il conflitto, la rinnovata enfasi sulla sovranità e sul diritto di uno Stato di governarsi senza interferenze esterne – fra queste, in molti includono la Rete.

Quattro paesi – Russia, Cina, Iran e Corea del Nord – sono in lotta con gli Stati Uniti. L'antipatia verso il momento unipolare, il desiderio di disfare l'architettura internazionale americanocentrica e l'obiettivo di raggiungere il dominio regionale hanno condotto i nostri oppositori a sviluppare strategie, tattiche e tecnologie per frustrare il potere statunitense. Ma lo scontro ha assunto nuove forme che hanno colto di sorpresa la superpotenza. Non è una guerra convenzionale. I nostri oppositori non hanno rinunciato all'uso della forza o alla coercizione, ma lo fanno in modo più scaltro per evitare una guerra conclamata contro l'America. Il ciber-spazio è diventato il campo di battaglia preferito. Gli Stati usano Internet per scopi

coercitivi, sfruttando gli attributi della Rete: un relativo anonimato, un certo grado di possibilità di negare il proprio coinvolgimento, i potenti effetti cognitivi garantiti dalle tecnologie informatiche, la loro portata globale. Le attività dei nostri rivali occupano un'area grigia fra la pace e la guerra, nella quale Washington e i suoi alleati, incapaci di rispondere con la forza, hanno trovato spesso e volentieri ostacoli a condurre efficaci rappresaglie.

A essere onesti, molte operazioni dei nostri oppositori avevano natura difensiva, essendo iniziate in risposta ai distratti tentativi degli Stati Uniti di promuovere la democrazia di mercato dopo la guerra fredda. Internet ha portato idee e aspettative in nazioni precedentemente isolate e, di conseguenza, i nostri rivali si sono dotati di una narrazione che dipingeva come ostili gli intenti di Washington, volti al cambio di regime e potenziati dalle ong, dai social media e in generale da quello che i russi chiamano «dominio dello spazio informativo». Ora sono invece passati all'offensiva.

Una quota troppo ampia del dibattito sul ruolo dello spazio cibernetico in questo conflitto ruota attorno al precedente della guerra nucleare. Quest'ultima minacciava catastrofi. L'apocalisse cibernetica è però improbabile. Un grande ciberattacco difficilmente è in grado di produrre un colpo decisivo e può scatenare una rappresaglia atomica. In breve, il gioco non vale la candela. Le operazioni cibernetiche forniscono un nuovo modo per ottenere vantaggi militari e forse strategici, ma ciò non risulterà dal solo equivalente digitale di un disastro nucleare. Semmai, gli effetti cibernetici più interessanti sono la manipolazione dei software, dei dati, della conoscenza, delle opinioni. L'obiettivo non è cinetico, ma cognitivo, l'alterazione delle informazioni per cambiare pensieri e comportamenti. Essenzialmente, lo scopo strategico è inficiare il morale, la coesione, la stabilità politica e, in ultima istanza, diminuire la volontà dell'oppositore di resistere. Questo tipo di operazione fornisce la possibilità di ottenere risultati coercitivi senza correre il rischio di innescare una guerra conclamata e restando sotto la soglia dell'accettabilità, minimizzando le probabilità di un'escalation. La manipolazione delle informazioni e del processo decisionale aggiungerà ulteriore complessità a ogni conflitto, fornirà vantaggi militari e sfiderà le nostre strategie convenzionali di impiego della forza bruta. Queste capacità verranno perciò impiegate da Russia, Cina, Iran e Corea del Nord per colpire gli Stati Uniti sottraendosi alla nostra superiore capacità di infliggere punizioni.

2. La prima «rivoluzione della conoscenza» creata dall'invenzione della stampa ha innescato secoli di tumulti politici. Le tecnologie digitali hanno lo stesso effetto, ma a un ritmo più veloce e con conseguenze più ramificate.

Internet sta accelerando tendenze politiche più generali che stanno a loro volta ridefinendo il ruolo dello Stato, l'efficacia della liberaldemocrazia e l'autorità dei valori dell'illuminismo centrati sul primato dell'individuo. Questi valori si confrontano ora con potenti sfide ideologiche da parte di regimi autoritari in un'epoca in cui molti cittadini delle stesse nazioni occidentali sono consumati dal dubbio. In

molte regioni del mondo viene messo in discussione l'ideale occidentale del progresso e della perfettibilità. Le nuove tecnologie forniscono all'opinione pubblica interna e agli oppositori stranieri un veicolo ideale per questa operazione. Intaccando così la narrazione politica dominante della democrazia di mercato, essa stessa già in grossa difficoltà a causa delle proprie lacune e dei ripetuti sforzi dei regimi autoritari per indebolirla.

Internet ha cambiato i requisiti per la legittimazione e il consenso. Affinché un governo sia percepito come legittimo dai propri cittadini c'è bisogno di qualcosa di più dei meccanismi della democrazia rappresentativa. Quest'ultima, per com'è ora strutturata, non soddisfa le aspettative dei cittadini create dalla Rete, fra cui figurano l'accesso alle informazioni e il coinvolgimento diretto nel processo decisionale. Sono le stesse pressioni subite dagli ambienti economici a adottare organizzazioni più piatte, meno gerarchiche. Se i governi democratici vorranno ricostruire la propria legittimità, la politica e il diritto si dovranno evolvere per tenere conto dell'evoluzione delle aspettative. Non è ancora chiaro quale forma assumeranno questi nuovi meccanismi, ma di certo richiederanno maggiore trasparenza e partecipazione diretta.

Tutti i paesi vengono politicamente sfidati da Internet. Le democrazie non ne sono immuni e si confrontano con problemi immediati, ma nel lungo periodo la minaccia più seria ed esistenziale delle tecnologie informatiche è diretta ai regimi autoritari, che faticano a gestirla. I governi illiberali, caratterizzati da brusche relazioni con i propri cittadini, hanno reagito restringendo l'accesso alle informazioni, fornendo contronarrazioni e creando sistemi ubiqui di sorveglianza per mantenere il controllo.

Internet si sta democratizzando, se con questa espressione intendiamo una maggiore partecipazione e non un'adesione ai valori politici democratici. I gruppi estremisti che rigettano gli ideali liberali sono fra i beneficiari della «democratizzazione» della conoscenza e della comunicazione. Nel lungo periodo – forse decenni – un maggiore accesso alle informazioni e una maggiore partecipazione potrebbero espandere la democrazia liberale, ma l'effetto politico immediato della Rete è stato di rivitalizzare le visioni estreme e aumentare il numero di chi le condivide¹.

Le conseguenze più pronunciate si hanno sulla mediazione dei contenuti, con media decentralizzati aperti a milioni di utenti che si sostituiscono ai redattori e ai *fact checkers* del passato. Negli anni Sessanta, Daniel Moynihan sosteneva che a chiunque era consentito avere la propria opinione ma non la propria versione dei fatti. Internet permette a ciascuno di avere i propri fatti. I social media amplificano questa tendenza. Facebook è diventato fonte primaria di notizie per la maggioranza degli americani, ma la sua struttura fatta di «amici» e «like» implica che le informazioni presentate possono essere adattate alle preferenze di gruppo. I russi sono stati molto astuti nello sfruttare questa caratteristica per plasmare le opinioni di certi segmenti popolari occidentali. Mentre i cinesi la impiegano per imporre il

1. Per una discussione pionieristica che risale a fine anni Novanta, si veda J. SULER, «The Psychology of Cyberspace», goo.gl/fo6c5D

conformismo nei dibattiti online – non solo in patria, visti i tentativi in tal senso per esempio in Australia.

3. In presenza di determinate condizioni – impopolarità del regime autoritario, oppositori carismatici, un incidente che faccia da innesco – le tecnologie informatiche forniscono uno strumento per trasformare il dissenso in azione. Cina, Russia e Iran temono questo scenario stile «primavera araba». Il primo ministro russo Medvedev ha sostenuto che le rivolte arabe sono state istigate da forze occidentali che stavano cospirando anche per rovesciare il governo di Mosca: «Guardiamo in faccia la realtà. Stavano preparando uno scenario simile per noi e ora proveranno ancora di più a implementarlo»².

L'informazione è una minaccia per i regimi autoritari, difettando questi ultimi dei meccanismi democratici per accomodare il dissenso e le pressioni per le riforme politiche. Ciò li conduce a reagire a quella che percepiscono come un'egemonia informativa dell'Occidente. Ma non possono scommettere solo sulla risurrezione del nazionalismo in difesa dell'autoritarismo, perché il suo richiamo è parziale e crea dinamiche imprevedibili. In particolare, la dirigenza cinese teme che i sentimenti nazionalisti impiegati per mantenere il sostegno popolare finiscano fuori controllo. Così, Russia, Cina, Iran e Corea del Nord stanno creando una potente contronarrazione fatta di nazionalismo eroico, di indomabile ostilità occidentale e di ipocrisia americana, usando la censura e il dominio sui media nazionali per negare ai propri cittadini l'accesso a informazioni provenienti dall'Occidente potenzialmente distruttive.

Il disagio nei confronti della centralità narrativa dei media occidentali ha spinto Mosca e Pechino a provare a emularli, creando concorrenti come Russia Today che, con i suoi canali in spagnolo e arabo, dà un taglio fortemente antiamericano e filorusso alle notizie. La stessa emittente sfrutta le gerarchizzazioni di Google per far apparire i propri articoli fra i primi risultati delle ricerche³. Il presidente Putin ha definito l'azienda proprietaria di questa televisione, Novosti, organizzazione di importanza strategica per la Russia.

La Cina risponde con diversi media di Stato. Il *Global Times* è stato riprogrammato nel 2009 per promuovere presso un pubblico di lingua inglese una più positiva immagine della Repubblica Popolare assieme a opinioni talvolta stridule e antiamericane. China Central Television si è aperta a un pubblico internazionale nel 1996 e offre ora servizi in otto importanti idiomi, con l'esplicito scopo di creare una narrazione migliore di ciò che accade nel paese. Entità sostenute dallo Stato hanno acquistato testate come il *South China Morning Post* e hanno cominciato a conformarne le politiche editoriali. I dirigenti di Alibaba sostengono che il loro obiettivo è di «migliorare l'immagine della Cina e offrire un'alternativa alle pregiudizievole lenti degli organi di stampa occidentali»⁴.

2. N. ABDULLAEV, «Kremlin Sees Peril in Arab Unrest», *The Moscow Times*, 24/2/2011.

3. K. WADDELL, «Kremlin-Sponsored News Does Really Well on Google», *The Atlantic*, 25/1/2017.

4. D. BARBOZA, «Alibaba Buying South China Morning Post, Aiming to Influence Media», *The New York Times*, 11/12/2015.

Queste acquisizioni hanno ingenerato un certo grado di autocensura fra le imprese occidentali per non perdere l'accesso al mercato cinese. Quanto invece siano riuscite a cambiare le opinioni straniere sulla Repubblica Popolare è un altro discorso. Parimenti incerti i risultati degli Istituti Confucio, goffo tentativo di dotarsi di *soft power* negli Stati Uniti, dove la maggior parte di queste entità è sorta, subito attirandosi critiche da varie direzioni senza un apprezzabile miglioramento delle opinioni americane sulla Cina ⁵. Il problema di Pechino resta lo stesso del 1926, quando un dissidente di punta, Lu Xun, scrisse: «Le menzogne scritte con l'inchiostro non possono mai nascondere fatti scritti col sangue».

Sia la Cina che la Russia usano troll su Internet per plasmare i social media in modi favorevoli ai propri regimi e dannosi per gli Stati Uniti e per altri oppositori. Pechino si concentra soprattutto entro i propri confini, mentre i troll russi cercano influenza anche presso pubblici stranieri. Mosca è stata abile nello sfruttare i social network occidentali e ha automatizzato con successo questa pratica attraverso l'uso di *chatbots*, programmi che simulano un utente reale nelle discussioni online per amplificare ed estendere la portata della propaganda. Prima del 2017 un misto di indifferenza aziendale e scarsa supervisione ha dato a questi strumenti ampia libertà. Inoltre, Russia e Cina sfruttano le garanzie democratiche come la libertà di espressione per massimizzare l'accesso agli utenti occidentali con pubblicità a tutta pagina o persino inserti sponsorizzati, operazioni che durante la guerra fredda sarebbero state impensabili.

Altri oppositori come Iran e Corea del Nord condividono il disgusto nei confronti del dominio mediatico occidentale, ma i loro sforzi si concentrano sul pubblico domestico. L'obiettivo primario è controllare la propria gente più che persuadere utenti stranieri. Tuttavia, gli sforzi per isolare completamente le reti nazionali – che in Cina arrivano a costruire industrie locali per produrre tecnologie indigene – condividono una fondamentale debolezza. Tutti questi paesi, Corea del Nord inclusa, desiderano una qualche forma di connessione con il mondo esterno, anche solo per scopi pecuniari. Non c'è solo Internet: anche il turismo, l'intrattenimento d'importazione clandestina, l'istruzione all'estero offrono un modo alle popolazioni locali per accedere a informazioni potenzialmente dirompenti e per minare la narrazione di Stato. Gli effetti politici immediati possono essere contenuti, ma la loro gradualità può corrodere l'autoritarismo.

4. Cina, Russia, Iran e (in misura minore) Corea del Nord hanno capacità militari cibernetiche ben sviluppate. Qualora dovessimo scontrarci apertamente con loro, dovremmo aspettarci cyberoperazioni abbinate alla guerra elettronica, ad attacchi antisatellitari, a campagne propagandistiche e ad altre tattiche e armi non convenzionali. L'intento sarà sempre quello di diminuire il «vantaggio informativo» americano attaccando i mezzi di comunicazione e gli asset di intelligence, ricognizione e sorveglianza. Oltre a rallentare e danneggiare il processo decisionale statu-

5. E. REDDEN, «New Scrutiny for Confucius Institutes», *Inside Higher Ed*, 26/4/2017; R. WIKE, «6 Facts About How Americans and Chinese See Each Other», Pew Research Center, 30/3/2016.

nitense e a creare incertezze, tumulti e dissensi politici.

Negli ultimi dieci anni, di fronte alle sfide delle tecnologie informatiche, Mosca è passata da un approccio difensivo a uno attivo, andando all'attacco. I russi hanno applicato ai nuovi strumenti le classiche tecniche di disinformazione in cui eccellono da sempre, usando troll, *fake news* e rivelazioni scottanti contro gli oppositori domestici nei primi anni dell'era Putin. Poi, hanno rivolto le stesse armi contro l'Occidente, adottando tattiche che compensassero le loro debolezze. L'obiettivo è rimodellare le opinioni occidentali attraverso i propri media, centinaia di troll per disseminare messaggi filorussi nelle sezioni dei commenti dei siti occidentali, *chatbots* per inondare di ostilità i social media e, ovviamente, rivelazioni politicamente dannose estorte tramite varie organizzazioni tra cui WikiLeaks. La guerra di nuova generazione sarà dominata dall'informazione e dalle operazioni psicologiche volte a deprimere il morale del personale in divisa e della popolazione dell'avversario. Gli strateghi russi definiscono l'informazione un'arma e la impiegano contro gli Stati Uniti e i loro alleati per minacciare, manipolare, forzare. La dottrina militare russa del 2014 prescrive di «esercitare pressione simultanea sul nemico in tutto il suo territorio e nello spazio informativo globale».

Mosca si avvantaggerà sia dei travagli delle democrazie liberali occidentali sia degli impulsi estremisti di Internet. Occorre comunque ribadire che, per quanto astuti, gli sforzi russi sarebbero molto meno efficaci in assenza delle più ampie tendenze politico-tecnologiche in atto nei paesi che la Russia ha messo nel mirino. I russi sanno che l'adesione occidentale alla libertà di espressione ostacola lo sviluppo di anticorpi alla loro campagna di disinformazione. Nessuno in America o in altre democrazie vuole che il governo censuri Internet – i nostri avversari invece non si fanno scrupoli. Il Cremlino ha una lunga esperienza con questo tipo di pratiche: alcuni dei trucchi impiegati nelle elezioni statunitensi del 2016 risalgono al tempo degli zar. Ma né Washington né i suoi alleati avevano la più pallida idea di come difendersi o rispondere a questo intento coercitivo. L'effetto desiderato dai russi è di tipo cognitivo: raggiungere obiettivi politici senza usare la forza militare. Valerij Gerasimov, il capo di Stato maggiore delle Forze armate, ha detto che «le stesse regole della guerra sono cambiate significativamente, le opzioni non militari rivestono un ruolo maggiore nel raggiungere obiettivi politici e strategici e, in certe situazioni, hanno un potere molto superiore a quello delle armi»⁶. Controllo riflessivo, lo chiamano i russi⁷.

Gli sforzi di Mosca non sono la causa primaria dei danni alla legittimità e alle istituzioni occidentali, che invece sono autoinflitti, essendo il risultato di disuguaglianze crescenti e di un generale scontento nei confronti del ritmo e della direzione del cambiamento sociale. La Russia sfrutta e amplifica le tendenze esistenti attingendo ai successi dei propri servizi d'intelligence in campo disinformativo – dai Proto-

6. M. CONNELL, S. VOGLER, «Russia's Approach to Cyber Warfare», *CNA Analysis & Solutions*, 16/9/2016; N. FEDYK, «Russian "New Generation" Warfare: Theory, Practice, and Lessons for U.S. Strategists», *Small Wars Journal*.

7. T.L. THOMAS, «Russia's Reflexive Control Theory and the Military», *The Journal of Slavic Military Studies*, vol. 17, n. 2, 2004, pp. 237-256.

colli dei Savi di Sion alla fandonia sull'Operazione Infektion (i laboratori militari americani avrebbero creato l'Aids). Già il *long telegram* di George Kennan del 1946 metteva in guardia dagli sforzi sovietici per fomentare le divisioni, intaccare la fiducia e creare sussulti nelle nazioni occidentali. E proprio come quando cercò durante la guerra fredda di usare elementi democratici progressisti, oggi Mosca guarda ai gruppi nazionalisti di estrema destra come potenziali alleati e agenti d'influenza⁸. Di diverso ci sono la velocità e lo scopo della disseminazione, il potere dei nuovi strumenti d'informazione e la facilità di accesso ai segmenti popolari suscettibili⁹.

Gli sforzi della Cina sono concentrati primariamente sulla sua popolazione e sulla diaspora. La propaganda di Pechino è stata molto efficace nel persuadere il mondo dell'inevitabile ascesa economica cinese e nell'esporre le lacune degli Stati Uniti. Tuttavia non è riuscita a rendere attraente la cultura del partito unico. La Repubblica Popolare ha aderito alla strategia del *soft power* dieci anni fa, quando Hu Jintao invocava una «ideologia socialista più affascinante e unificante». I funzionari di partito vogliono fare del paese una «locomotiva del dibattito» così com'è una potenza in campo economico¹⁰. Ma sarà difficile raggiungere l'obiettivo. Le aspirazioni sono frenate dagli aspri rapporti con i vicini, dalla repressione domestica e dalle inerenti contraddizioni del sistema politico.

La dottrina cinese per l'uso militare dello spazio cibernetico è più convenzionale rispetto a quella russa. Punta a inficiare le prestazioni degli armamenti e le funzioni di comando. Fonti giornalistiche riportano come dal 2001 più di una ventina di importanti sistemi d'arma americani siano stati compromessi, compresi aerei, difese antimissile e testate nucleari. La Cina ha attivato tali operazioni di intrusione per capire i limiti operativi degli armamenti statunitensi, copiarli e prepararsi a interferire in caso di combattimento.

Iran e Corea del Nord usano le ciberoperazioni a scopi coercitivi e punitivi contro banche o aziende dell'intrattenimento come Sony o Sands Casino. Ma il loro non è un obiettivo distruttivo e l'intento potrebbe anche essere solo quello di mostrare a sé stessi e alla propria gente di poter stuzzicare impunemente l'aquila. Vale la pena notare come nessuno di questi paesi parli di attaccare le infrastrutture vitali per produrre una «Pearl Harbor cibernetica». Benché questi argomenti, al pari dell'idea di un attacco da parte di un attore non statuale, siano il pilastro del dibattito sulla cbersicurezza negli Stati Uniti, non c'è alcuna evidenza a supportarli. La discussione pubblica non riflette la realtà dei conflitti cibernetici.

5. Benché entrambe efficaci entro i propri confini e, in particolare i russi, nel danneggiare i processi elettorali occidentali, né Mosca né Pechino sono state in grado di sviluppare alternative attraenti alle democrazie liberali. La narrazione razional-nazionalista di Putin si ferma alle popolazioni slave e ai gruppi di estrema

8. www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/6-6.pdf

9. T. BOHARDT, «Operation INFEKTION: Soviet Blog Intelligence and Its AIDS Disinformation Campaign», *Studies in Intelligence*, vol. 53, n. 4, dicembre 2009.

10 goo.gl/kac1B9

destra, perché la retorica ostile, le azioni repressive e la corruzione della Russia minano i tentativi di sedurre pubblici stranieri più ampi. Similmente poco persuasive sono le descrizioni adulatorie di Xi Jinping. Entrambe le potenze lottano senza successo contro impressioni negative largamente condivise a livello internazionale. Per esempio, due terzi delle persone intervistate in un recente sondaggio globale esprimevano commenti sfavorevoli nei confronti della Russia¹¹. Indice del fatto che Russia Today e compagnia non hanno forse mietuto tutti questi successi.

L'idea russo-cinese di imbrigliare gli Stati Uniti, sostituire l'ordine mondiale post-1945 e ridare enfasi alla sovranità suscita l'interesse di molte nazioni nel G77 e nel movimento dei non allineati, ma Mosca e Pechino non sono ancora state capaci di trasformare questo interesse in autentico sostegno per creare nuove istituzioni. Il consorzio dei Brics è un intelligente riconoscimento del cangiante equilibrio di potenza al di fuori dell'ambito transatlantico, ma una profonda faglia attraversa le nazioni che lo compongono: India e Brasile hanno idee molto diverse da Russia e Cina nei confronti della libertà d'espressione.

La Conferenza mondiale per le comunicazioni internazionali del 2012 vide le proposte russe per riscrivere la gestione di Internet ricevere il sostegno della maggioranza dei partecipanti. Tuttavia, più che a una genuina adesione alla proposta specifica, può anche darsi che ciò fosse dovuto più a un'opposizione al pensiero occidentale, ancorato alla difesa dello status quo e all'enfasi sulla Rete «libera e aperta». Anche perché Mosca si trovò isolata appena due anni più tardi alla conferenza NetMundial, con la sua agenda politica sostenuta solo da Cuba e (forse per errore) dall'India. I più efficaci strumenti d'influenza per Russia e Cina sono dunque un mix di coercizione e incentivi monetari.

6. È stato un errore assumere che il tramonto della guerra fredda avrebbe implicato il trionfo delle democrazie di mercato e la fine dei conflitti e delle competizioni fra gli Stati. Washington si trova in un mondo in cui il proprio *soft power* è diminuito e quello *hard* è meno utile. Le potenze emergenti si percepiscono come concorrenti per il potere economico, l'influenza internazionale e il primato regionale. Alcune sono pure passate dalla sfida al conflitto. In questo ambiente, i nostri oppositori sfrutteranno le opportunità create dalle tecnologie informatiche per danneggiare l'America e avanzare il proprio interesse nazionale.

Siamo in un nuovo tipo di conflitto al cui centro ci sono le informazioni e gli effetti cognitivi da esse prodotti. Benché la gara favorisca in teoria gli Stati Uniti e l'Occidente, per acquisire un vantaggio occorre ripensare idee, strategie e narrazioni. I principi intellettuali dell'approccio americano – democrazia e Stato di diritto – restano forti, ma abbisognano di essere riarticolati per restare persuasivi. Il *soft power* a stelle e strisce scaturiva da idee efficaci, che però sono state minate dagli interrogatori della Cia, dalle rivelazioni di Edward Snowden e da quasi due decenni di disavventure in Medio Oriente. Le azioni degli Stati Uniti negli ultimi

15 anni vengono ora percepite in modo molto meno benigno. L'invasione dell'Iraq nel 2003 – senza l'approvazione del Consiglio di Sicurezza delle Nazioni Unite, punto cruciale per molti paesi che vedono nell'Onu un modo per imbrigliare l'altrimenti illimitato potere degli Stati più grandi – sembra aver inacidito le opinioni sull'America al punto da non rendere più sufficiente un'affinità per la cultura popolare statunitense.

Siamo in un mondo post-1945 e ciò ha vaste conseguenze politiche. Prima di quell'anno, i governi recitavano un ruolo più definito sia internamente che internazionalmente. Alcuni preferirebbero tornare alla definizione tradizionale di sovranità, in virtù della quale i diritti universali erano meno importanti. Il modello occidentale di gestione della politica, basato sulla democrazia parlamentare e rappresentativa e sulle norme dell'illuminismo a essa associate, non assicura più il consenso dei governati.

Gli approcci governativi e multilaterali sviluppati in Occidente in risposta alle crisi globali degli anni Trenta non sono più adeguati a incontrare le aspettative dei cittadini, rimodellate in buona parte dalle tecnologie informatiche e da Internet. Tuttavia, le alternative all'ordine post-1945 – sovrani autoritari e assoluti o nebulose *governance* multilivello – sono ancora meno attraenti. Occorre riformare ciò che già abbiamo. Finché un nuovo modello di organizzazione politica non andrà incontro alle tecnologie dell'informazione e non imparerà a incanalare i loro effetti politici, lo spazio cibernetico resterà un'arena che i nostri oppositori sfrutteranno ben volentieri.*


(traduzione di Federico Petroni)

* Una versione di questo articolo è apparsa il 26/9/2018 sul sito del Center for Strategic and International Studies sotto il titolo «Cognitive Effects and State Conflict in Cyberspace».

LE CONSEGUENZE ININTENZIONALI DELLE FAKE NEWS

di Simon *TEMPLAR*

Regimi di ogni natura agitano la minaccia di notizie false per ostacolare l'accesso dei cittadini alle informazioni. Il vero pericolo è la mancanza di fiducia dei governanti nelle capacità di discernimento dei governati. Il caso Macron e l'eredità di Trump.

1.  RA I DETRITI DELLA FAZIOSITÀ POLITICA capita spesso di imbattersi nella legge delle conseguenze inintenzionali, come già accaduto nella prima parte del mandato del presidente americano Donald Trump. La più importante, e impreveduta, di queste conseguenze è stato l'impatto globale dei commenti di Trump sul fenomeno delle cosiddette *fake news*. A ben vedere, il fatto stesso che ci siano state conseguenze di natura globale è l'epitome dell'inintenzionale, dal momento che Trump non ha mai avuto una strategia che andasse al di là del puntellamento del sostegno della sua base elettorale e della fustigazione dei media americani mainstream che considera prevenuti nei suoi confronti.

Altrettanto emblematico è il fatto che nonostante molte organizzazioni che si occupano della difesa della libertà di stampa lo abbiano messo in guardia circa le conseguenze potenzialmente letali delle sue affermazioni, Trump sembri tenere in considerazione unicamente l'aspetto narcisista del problema. Il presidente americano è orgoglioso del fatto che una sua frase divenga popolare nel mondo intero, mentre trascura il fatto che questa popolarità sia dovuta alla repressione delle libertà d'espressione e di stampa da parte delle potenze autocratiche¹. Sempre resiliente nei confronti delle critiche, anche se paradossalmente ipersensibile, Trump fa finta di non vedere che gli Stati Uniti sono precipitati al quarantacinquesimo posto nella classifica dell'indice della libertà di stampa a causa della sua retorica contro i media. Per quanto non sia possibile provare un legame causale tra i due fenomeni, sembra esserci un forte rapporto di correlazione inversa tra questo rapido declino e l'aumento degli arresti e delle molestie fisiche nei confronti dei giornalisti in tutto il mondo².

1. J. SCHWARTZ, «Trump's "Fake News" Rhetoric Crops up Around the Globe», *Politico*, 30/7/2018, goo.gl/uUphWV

2. *Ibidem*.

L'avvisaglia più evidente del fatto che le *fake news* siano qualcosa di più di una moda politica passeggera destinata a finire nella discarica della storia è l'esempio inquietante di leader di paesi democratici che cedono alla tentazione di usarle come arma. Per chi studia la corruzione politica e la repressione, è tutt'altro che sorprendente osservare che paesi che aderiscono alle istituzioni democratiche solo a parole stiano sfruttando questo fenomeno. È però quando leader come il francese Emmanuel Macron, presidente di un paese ritenuto un faro di democrazia e stabilità, riescono a far approvare dal parlamento una legge che autorizza il governo a prendere misure d'emergenza per bloccare «informazioni manipolatorie e fuorvianti» entro quarantott'ore dalla sottoposizione delle stesse alla magistratura, e la cui validità è limitata ai tre mesi precedenti alle elezioni generali, che dobbiamo riconoscere di avere un problema³.

Macron ritiene di essere stato vittima, nel 2017, di una campagna di disinformazione feroce e ingannevole ordita dai suoi oppositori politici. Avendo limitato il lasso temporale in cui la legge produce i suoi effetti (il periodo immediatamente precedente alle elezioni) e previsto che le informazioni potenzialmente oggetto dell'azione governativa debbano essere sottoposte all'attenzione della magistratura, la Francia è sicura di aver individuato una ragionevole «via di mezzo aurea» per farsi strada nel dibattito sulle *fake news*. E se rispetto alle iniziative cui hanno dato vita paesi come Malaysia, Brasile o Kenya queste sono solo frenate parziali, la realtà è che la legge francese in materia di *fake news* potrebbe finire per creare le sue stesse conseguenze inintenzionali, dal momento che azioni di questo tipo non permettono più di considerare la questione come un «fenomeno da dittatori» che viene manipolato per propositi personali. Macron ha ora conferito ai paesi democratici la flessibilità necessaria per replicare queste iniziative non democratiche.

2. A ben vedere, tuttavia, le peggiori conseguenze inintenzionali delle *fake news* provengono da una lunga lista di sospetti, alcuni soliti altri meno. Se è ancora impossibile stabilire quali saranno le ripercussioni ultime di tali iniziative, non è troppo presto per tracciare un resoconto che dia l'idea di quanto pervasive siano diventate queste misure in paesi autocratici, semiautocratici e persino democratici⁴.

- La Bielorussia ha approvato delle leggi che permettono al governo di perseguire persone che hanno diffuso «informazioni false sulla Rete» e, potenzialmente, di bloccare siti Internet che si ritiene abbiano violato le norme.

- Il ministero belga per l'Agenda digitale ha lanciato due iniziative che mirano specificamente a contenere la disinformazione sulla Rete.

- La polizia federale del Brasile ha annunciato la creazione di una task force speciale per identificare, localizzare e punire gli autori delle *fake news*.

3. R. HARIDY, «Opinion: How Fake News Is Being Co-Opted By Governments Around the World to Suppress Dissent», *New Atlas*, 4/8/2018, goo.gl/wUdKJo

4. D. FUNKE, «A Guide to Anti-Misinformation Actions Around the World», *Poynter*, 25/9/2018, goo.gl/DR8RcP

- Nelle settimane che precedevano le elezioni nazionali, il governo della Cambogia ha approvato delle misure che lo autorizzano a bloccare siti Internet e altri media considerati «un pericolo per la sicurezza nazionale».

- La Croazia ha approvato una legge intesa a fermare la diffusione dell'incitamento all'odio e della disinformazione sui social media.

- Il governo egiziano disciplina tutti gli account sui social media che hanno un ampio seguito al fine di assicurarsi che nel paese non vengano diffuse informazioni false.

- L'Indonesia ha creato un'Agenzia nazionale cibernetica e per il criptaggio incaricata di aiutare l'intelligence e la polizia nel combattere la disinformazione sulla Rete e le bufale sui social media.

- L'Italia ha istituito un portale online che i cittadini possono usare per informare la polizia di casi di disinformazione o di *fake news* diffuse sui social media.

- Il governo del Kenya ha approvato leggi che criminalizzano 17 diverse forme di attività sul Web.

- Nonostante sia il bersaglio abituale delle critiche sull'uso strumentale delle *fake news*, anche la Russia ha introdotto una legislazione sulla disinformazione.

- Presso l'Assemblea nazionale della Corea del Sud giacciono una dozzina di proposte in attesa di approvazione sulla limitazione/eliminazione della disinformazione online.

- Taiwan sta valutando l'aggiunta alla legge sul mantenimento dell'ordine sociale di una clausola che criminalizza la divulgazione di informazioni false.

- Il governo della Tanzania, sempre più preoccupato per la diffusione della disinformazione sulla Rete, ha applicato diverse iniziative giuridiche al fine di impedire la pubblicazione di *fake news* e/o punire coloro che le pubblicano.

- Con una mossa vagamente simile a quella della Tanzania, il governo dell'Uganda ha introdotto una tassa sull'uso delle piattaforme social da parte dei cittadini.

Seppure incompleta, questa lista illustra la tendenza globale dei governi a cercare di regolare, monitorare, limitare e restringere la partecipazione sociale e politica dei cittadini sulla Rete⁵. La maggior parte dei governi che ha introdotto questo tipo di misure restrittive ha tenuto a mettere in chiaro alle proprie opinioni pubbliche e all'intera comunità globale che tali iniziative vengono attuate «in nome del popolo», per aiutare le persone a districarsi meglio nel complicato mondo delle tecnologie di comunicazione nel quale viviamo. Cinici e scettici hanno più di qualche buona ragione per ignorare del tutto queste ipotetiche motivazioni altruistiche, perché nonostante la miriade di modi diversi con cui le nazioni stanno combattendo il presunto assalto delle *fake news* ci sono inquietanti problemi strutturali trasversali a tutte queste iniziative giuridiche.

3. Apparentemente, nessuno ha mai tentato di definire in modo esplicito che cosa siano le *fake news*. Impiegare termini amorfi e ambigui consente ai governi di

5. *Ibidem*.

usare a proprio vantaggio la cosiddetta «fallacia della brutta china» (*slippery slope approach*) nei confronti delle forze di opposizione: se ti metti contro di me, farò in modo che i tuoi argomenti siano bollati come *fake news*. Si tende dunque a creare una commistione tra siti Internet che possono essere considerati a buon diritto sospetti e siti che mirano legittimamente a fornire informazioni alternative a quelle dei media di Stato.

Lo scopo delle iniziative governative non è quindi quello di rivelare ai cittadini la manipolazione delle notizie, ma di limitare il loro accesso a informazioni non in sintonia con quelle diffuse dai canali ufficiali. La maggior parte di queste misure non sembra scaturire dalla necessità di migliorare la qualità delle notizie e delle informazioni, bensì dalla volontà di creare ostacoli e barriere giuridiche insormontabili alle organizzazioni di base che non intendono adeguarsi alle prescrizioni delle autorità centrali. Molte delle leggi sulle *fake news* non sono altro che progetti malcelati per prevenire un sano sviluppo della società civile in paesi che ne hanno un disperato bisogno.

Alcune delle iniziative più benintenzionate che cercano di coinvolgere in modo intenso e diretto il pubblico nella regolamentazione delle *fake news* e nella conseguente punizione dei trasgressori potrebbero benissimo scoperchiare un vaso di Pandora che non unirebbe i cittadini ma incuneerebbe notevoli divisioni tra i gruppi sociali. Alcune di queste proposte di legge assomigliano in modo inquietante a un invito aperto a fare la spia sui propri vicini. Infine, non è certo un caso che in ogni singola circostanza, indipendentemente dalla natura del sistema o del regime politico del paese, non ci sia alcuna menzione delle ripercussioni e delle conseguenze sui governi o sui funzionari governativi nel caso in cui vengano giudicati colpevoli di aver diffuso *fake news*. Questa definizione a senso unico degli autori del reato è estranea alla realtà, dal momento che i peggiori artefici e diffusori delle *fake news* sono spesso gli stessi governi.

Se prendiamo per buono quest'ultimo assunto, non possiamo che giungere a una conclusione particolarmente inquietante sulle iniziative legislative relative alle *fake news*: si tratta di tentativi volti non già a migliorare la qualità del dibattito politico, ma a distruggere la sua potenzialità. La conseguenza ultima del tentativo dei governi di usare le presunte *fake news* come armi per randellare gli oppositori e l'opposizione è dunque l'indebolimento della vigilanza pubblica, della possibilità dei cittadini di esprimere critiche e dell'attivismo di base. Negli Stati Uniti la gente guarda con perplessità alle filippiche di Trump contro le *fake news* principalmente a causa della sua persistente fiducia nelle istituzioni della democrazia americana e dei suoi principi congeniti che tutelano la libertà di stampa, di associazione e di pensiero. Fin qui, tutto bene. Ma molti altri governi, evidentemente ispirati dalla retorica trumpiana, non sono soggetti alle stesse limitazioni strutturali imposte dal sistema di pesi e contrappesi americano. Le loro iniziative, dunque, non rinforzano la qualità del dibattito politico del paese, ma solo il potere dei governi.

4. Malgrado tutti i problemi discussi finora, esiste un dilemma persino più significativo per coloro che vogliono concedere ai governi almeno il minimo beneficio del dubbio: è possibile che la conseguenza ultima del contributo inintenzionale dato da Trump alla questione delle *fake news* sia una crisi di fiducia nelle persone stesse? Se non vogliamo guardare a queste dinamiche inquietanti come a un tentativo cinico dei governi di controllare i loro cittadini e di ostacolare lo sviluppo di una vera competizione politica, dobbiamo allora fare i conti con il fatto che tali manovre politiche dimostrano quanta poca fiducia abbiano i governi nella capacità dei governati di discernere, valutare e giudicare la validità delle informazioni. Nelle democrazie veramente stabili gli elettori sono solitamente orgogliosi di eleggere leader nei quali hanno piena fiducia e si aspettano che nell'esercizio della leadership essi diano prova di carattere, integrità, professionalità e sincerità. Le iniziative relative alle *fake news* intraprese da paesi caratterizzati da sistemi e regimi politici molto diversi fra loro rivelano come i governi si comportino in modo opposto quando si tratta di giudicare i propri cittadini.

Perché mai i governi dovrebbero aver bisogno di promulgare leggi per bloccare le *fake news* quando inveiscono continuamente contro la loro insignificanza, ingannevolezza e debolezza? E perché dovrebbero percepire la necessità di impedire preventivamente che le *fake news* raggiungano le persone o di ostacolare l'esposizione dei propri cittadini alle stesse? I governi non fanno queste cose perché considerano le *fake news* un nemico straordinariamente potente che deve essere preso sul serio. Le iniziative dei governi segnalano la loro mancanza di fiducia nella capacità delle persone di discernere il vero dal falso, o comunque la loro riluttanza a dargli questa responsabilità in un'era in cui i media sono iperconnessi e la soglia d'attenzione iperlimitata.

Queste iniziative governative rispondono dunque a una logica per la quale le *fake news* raggiungono il loro obiettivo a causa della mentalità ristretta della gente comune, della sua pigrizia nell'acquisizione di conoscenza e della sua irresponsabilità quando si tratta di discernere la veridicità delle informazioni. Purtroppo, alcuni sondaggi suffragano questa visione ultrapessimista del pubblico⁶. I governi dicono di essere preoccupati dal fatto che la soglia media d'attenzione non superi i dieci secondi, dal poco tempo che le persone dedicano all'analisi accurata delle informazioni che leggono e dalla loro tendenza a leggere solo i titoli e non i contenuti. Ma le misure volte a contrastare le *fake news* non sono dirette ad armare meglio i cittadini, bensì a disarmarli completamente.

È questa la conseguenza ultima delle leggi contro la diffusione di informazioni false: le *fake news* non causeranno la morte della democrazia o il consolidamento dell'autocrazia, ma sono diventate il canale attraverso il quale i governi esibiscono la loro scarsa fiducia nelle qualità e nell'intelligenza dei cittadini. Il dibattito sul tema evolve dunque in una battaglia nella quale le persone percepiscono che i governi stanno cercando intenzionalmente di indebolirle, mentre questi ultimi si

6. T. EGAN, «The Eight-Second Attention Span», *The New York Times*, 22/1/2016, goo.gl/QfpO3d

sentono in diritto di fare precisamente ciò di cui vengono accusati. Questo, alla fine, potrebbe essere il lascito principale, e più odioso, della presidenza Trump: la vera disinformazione da combattere.

Perché le *fake news* non possono rovesciare un governo o distruggere una società, mentre la mancanza di fiducia e legittimazione reciproca tra governi e cittadini può certamente farlo.

(traduzione di Daniele Santoro)

PER UNA BIOGRAFIA GEOPOLITICA DI TELECOM

di *Alessandro ARESU*

L'infinita competizione intorno a una industria strategica italiana. Dal piano Rovati all'ingresso di Cassa depositi e prestiti, alla vittoriosa partita americana contro i francesi. Il caos della politica e la definizione della sicurezza nazionale.

*Quel che ora importa è di non compromettere
l'avvenire delle telecomunicazioni nazionali.*

Ernesto Rossi, 1953



1. EI PRIMI MESI DEL 2008, ANGELO ROVATI MI invitò a prendere un aperitivo con il mio maestro, Guido Rossi. Appuntamento alle sette al Four Seasons, a pochi passi dallo storico studio del professore, in via Sant'Andrea. Durante l'aperitivo tra i due giganti potevo solo ascoltare, ma mi interessava l'oggetto della conversazione. Sapevo che non avrebbero resistito: avrebbero parlato di Telecom.

In termini antropologici, Rovati si collocava in un filone entusiasta della «finanza bianca»: ci teneva a precisare la sua appartenenza («sono sempre stato democristiano»¹) e si impegnò sempre romanticamente per rifondare la Dc. Rossi, che per la sua vivacità intellettuale sfuggiva alle categorie, si poteva definire non solo un indipendente di sinistra, quale era stato da senatore, ma anche un «indipendente del partito di Mediobanca», se si considera la sua confidenza di lungo corso con i grandi giuristi di via dei Filodrammatici² e con lo stesso Enrico Cuccia.

Dopo qualche convenevole sulla situazione politica, Rovati cominciò subito a parlare dell'argomento che lo appassionava: il «suo» piano, il piano Rovati. Nonostante il piano lo avesse perseguitato, intrecciandosi con i suoi gravi problemi di salute, non poteva fare a meno di discuterne, soprattutto davanti al giurista che per due volte si era confrontato col problema Telecom, uscendone anch'egli provato, ma con poca voglia di parlarne³.

1. A. Rovati al XX Congresso della Democrazia cristiana, 19/11/2006, disponibile su Radio Radicale, goo.gl/Wmer7y

2. Si veda a questo proposito la toccante testimonianza di Rossi su Mignoli, G. Rossi, *Ariberto Mignoli, un uomo del diritto*, Mediobanca, 8/10/2014.

3. Credo che anche per il peso di Telecom Guido Rossi non abbia mai scritto il suo libro sulla storia del capitalismo italiano, richiestogli con insistenza da Roberto Calasso (R. CALASSO, «Guido Rossi citato a Londra e a New York», *Il Sole-24 Ore*, 20/3/2011).

Il piano era il documento dal titolo «Scorporo della rete di Telecom Italia. In-dirizzo industriale e considerazioni economico-finanziarie» (5 settembre 2006), in-viato da Angelo Rovati, al tempo consigliere economico del presidente del Consi-glio Romano Prodi, ai vertici dell'azienda telefonica, allora presieduta da Marco Tronchetti Provera⁴. Il documento, che suscitò feroci polemiche, mise in difficoltà il governo Prodi, portò Rovati alle dimissioni e Rossi alla presidenza di Telecom, aveva la pretesa di disegnare il futuro dell'azienda di telecomunicazioni. Un'azien-da totalmente privata. Che si chiamava Telecom Italia. Chi aveva la responsabilità di declinare il riferimento all'Italia, nel gruppo, e di definire i suoi confini? Rovati aveva scritto che «la situazione finanziaria e industriale relativa alla rete di Telecom rappresenta un rischio per il sistema paese», paventando gli effetti per il sistema bancario e il rischio di scalate ostili da parte di «investitori finanziari, anche esteri». Il campione di basket e imprenditore democristiano aveva suggerito alcune opzio-ni per affrontare la situazione debitoria e le esigenze delle infrastrutture della co-municazione, svelando la propria preferenza. Ovvero, lo spin-off della rete e la sua quotazione con un 70% di flottante, seguendo l'esempio della rete elettrica di Terna (quotata nel 2004), e coinvolgendo lo stesso azionista di riferimento di Terna dell'epoca (la Cassa depositi e prestiti), oltre ad altri investitori istituzionali italiani⁵. Lo scopo era raggiungere un 30% in grado di garantire «la società da eventuali sca-late di soggetti sgraditi, di qualche mafia finanziaria internazionale»⁶.

Rovati, riprendendo il piano dal vivo, oltre a scommettere qualunque cifra che sulla sua soluzione si sarebbe tornati in futuro, e che prima o poi Cassa depositi e prestiti avrebbe investito in Telecom, vi aggiungeva una postilla. Nei contenuti, il progetto puntava, nel lungo termine, a un'integrazione con Mediaset. Se la storia industriale di Telecom, nel passaggio della privatizzazione, cominciava con l'affi-damento alla famiglia Agnelli, Rovati invece pensava a Berlusconi. Per l'imprendi-tore delle telecomunicazioni per eccellenza era ora di scegliere: era più importante continuare a fare politica oppure impegnarsi in una grande realtà industriale, capa-ce di giungere a più vaste aggregazioni europee da una posizione di forza, magari superando le stesse resistenze che il suo gruppo aveva incontrato Oltralpe? Berlu-sconi⁷ affidò a un libro del 2007 di Bruno Vespa il suo commento sulla vicenda Telecom sotto il governo Prodi, definendola «un misto di diletterantismo, di arrogan-za e di statalismo», ma tornando sulla questione della nazionalità: «Tra i gestori te-lefonici, Wind è diventata egiziana, Omnitel è finita agli inglesi di Vodafone, la 3 è

4. Nella prospettiva della storia e del punto di vista di Pirelli, il piano è discusso a lungo da C. BELLA-VITE PELLEGRINI, *Pirelli. Innovazione e Passione. 1872-2015*, Bologna 2015, il Mulino, in particolare pp. 467-472.

5. Citazioni da M. SIDERI, «Rete Telecom sotto controllo pubblico», *Corriere della Sera*, 14/9/2006. Per dare un'idea dell'infinita storia degli effetti del «piano», riporto solo alcuni dei suoi riferimenti in anni successivi, da parte dello stesso giornalista sulla medesima testata: «Un piano da 1,4 miliardi per la banda larga lombarda», *Corriere della Sera*, 27/4/2010; «Rete Telecom, piano per lo scorporo con Authority e Cassa depositi», *Corriere della Sera*, 16/9/2012; «Internet veloce, incentivi e addio al rame», *Corriere della Sera*, 1/3/2015.

6. O. CARABINI, «Rovati: "Nessun complotto né mio né di Prodi"», *Il Sole-24 Ore*, 14/9/2007.

7. L'impegno di Berlusconi era stato suggerito anche da Cesare Romiti nel 2007: O. CARABINI, «L'atto di accusa di Romiti: "Capitalisti che non rischiano"», *Il Sole 24 Ore*, 15/4/2007.

cinese. Perdere anche la principale tra le società di telefonia significherebbe essersi fatti totalmente colonizzare»⁸.

Al Four Seasons, il professor Rossi sottolineava i forti limiti regolamentari e politici del piano Rovati, anche se apprezzava la sua capacità di guardare allo scenario dei prossimi decenni⁹. Entrambi parlavano di Telecom con dolore e con passione. Erano rimasti scottati dall'azienda, come altri protagonisti del nostro capitalismo, che torneranno nella sua storia. Oltre al vertice, centinaia, migliaia di persone appassionate di Telecom, anzitutto la sua forza lavoro. L'attenzione, l'ossessione, le polemiche sull'azienda non cessano mai, nel cercare di capire cosa significhi «Italia» nelle telecomunicazioni. Telecom, più di ogni altra impresa, racconta le incompiute dei sogni tecnologici italiani, i miracoli spezzati di un paese che, a fronte di grandi capacità scientifiche e ingegneristiche, di una cultura politecnica che forma ricercatori e manager, non compie i passaggi decisivi, perde numerose occasioni. Il romanzo *Libertà* di Jonathan Franzen ruota intorno al sofferto diario scritto dalla protagonista, intitolato «Sono stati commessi degli errori»¹⁰. È il manoscritto che i morti e i vivi della storia di Telecom non sono e non saranno capaci di scrivere, perché dovrebbero farlo insieme.

2. Nel 1993, al suo ritorno in Rai, Beppe Grillo tuonò contro Biagio Agnes, a lungo direttore generale della Rai, mostrando la sua foto in diretta: «Non sa i congiuntivi, non sa l'italiano, ed è presidente di una cosa che fattura migliaia di miliardi!»¹¹. Al tempo, Agnes era al vertice della holding delle comunicazioni Stet (Società torinese esercizi telefonici), e Grillo gli imputava le bollette stellari dell'144. Nei suoi discorsi su Stet e la telefonia, Grillo accentuava l'espressione «migliaia di miliardi», per evidenziare patrimonio e ricavi del gruppo. Il 9 giugno 1995, un altro passo: Grillo inaugurò un filone del governo d'impresa in Italia, partecipando a Torino all'assemblea Stet, grazie alla delega del fratello, inserito nel libro dei soci, e contestando l'operato dell'impresa. Nel 2010, introdusse il suo intervento all'assemblea dei soci Telecom con una nota crepuscolare: «Oggi sono venuto a cele-

8. S. Berlusconi in B. VESPA, *L'Italia spezzata*, Milano 2006, Mondadori.

9. La stessa prospettiva, d'altra parte, ritorna nella ricostruzione coerentemente avversa alla politica industriale effettuata da Franco De Benedetti anni dopo: «In un futuro che è già presente la connettività diventa una commodity, le telecom devono cercare altre fonti di reddito, per esempio integrandosi con produttori di contenuti» (F. DE BENEDETTI, *Scegliere i vincitori, salvare i perdenti*, Venezia 2016, Marsilio, p. 154).

10. «Mistakes were made», in J. FRANZEN, *Freedom*, New York 2010, Farrar, Straus & Giroux. Non esiste un testo di storia d'impresa che affronti in modo onnicomprensivo la vicenda Telecom, coinvolgendo tutti i testimoni. Occorre quindi tenere presente le versioni dei protagonisti italiani, tra cui R. COLANINNO con R. GIANOLA, *Primo tempo. Olivetti, Telecom, Piaggio: una storia privata di 10 anni del capitalismo italiano*, Milano 2006, Rizzoli, e C. BELLAVITE PELLEGRINI, *op. cit.*, oltre alla posizione dell'azienda, «Pirelli in Telecom Italia», goo.gl/mFH7Ds. Si vedano inoltre E. CISNETTO, *Il gioco dell'Opa*, Milano 2000, Sperling & Kupfer; G. ODDO, G. PONS, *L'affare Telecom*, Milano 2002, Sperling & Kupfer; M. MUCCHETTI, *Licenziare i padroni?*, Milano 2003, Feltrinelli; D. GIACALONE, *Razza corsara. I mercati mal controllati e la politica in fuga: il caso Telecom e la mala privatizzazione*, Soveria Mannelli 2004, Rubbettino; F. DE BENEDETTI, *op. cit.*; M.M. DECINA, *Goodbye Telecom. Dalla Privatizzazione a una Public Company. Antologia del ventennale 1997-2017*, Firenze 2017, goWare.

11. B. GRILLO, *Tutto il Grillo che conta. Dodici anni di monologhi, polemiche, censure*, Milano 2008, Feltrinelli, p. 33. Il video è disponibile su goo.gl/EC8GMK

brare i funerali di Telecom Italia. Ho il lutto al braccio. La ex prima azienda tecnologica del paese è finita. Ogni anno, da dieci anni, diventa più piccola, più marginale nel contesto internazionale»¹².

Quei quindici anni rappresentano una vita nella storia d'Italia, un'era geologica nella storia della tecnologia, se consideriamo l'ascesa dei giganti digitali americani e cinesi. Nel mentre, sulla vicenda Telecom si sono espressi studiosi¹³, giornalisti, protagonisti con le loro ricostruzioni, nonché i procedimenti giudiziari. Si è trattato di un «acceso dibattito in cui si è discusso di tutto a proposito e a sproposito», per riprendere le parole di Bernabé nel 2009. Oltre a questo, c'è anche un segno geopolitico, che può essere ripercorso attraverso le osservazioni di Vito Gamberale nella lezione del 2007 per la laurea honoris causa in Ingegneria delle Telecomunicazioni da parte dell'Università di Tor Vergata. Si tratta di uno dei più sferzanti documenti sul capitalismo italiano degli ultimi decenni e merita considerazione perché Gamberale è stato uno dei più grandi manager della costellazione Telecom¹⁴. Nella sua ricostruzione, il 1990 è l'anno in cui si decise di accelerare lo sviluppo delle telecomunicazioni in Italia. Lo stesso anno in cui Fiat vendette Telettra, importante società del settore, ai francesi di Alcatel, chiudendo la possibilità dell'integrazione con Italtel del gruppo Iri-Stet nel polo che era stato denominato Telit. Nel 1987 Fiat aveva rifiutato la candidatura al vertice della manager di Italtel Marisa Bellisario, non per una valutazione negativa sulla persona (prematuramente scomparsa nel 1988), ma per l'eccessiva interferenza politica da parte di Craxi in una società paritaria.

La vicenda viene ricordata da Ferruccio de Bortoli per sostenere la debolezza dei poteri italiani, incapaci di trovare un compromesso decente¹⁵. La fine della guerra fredda segnò un indebolimento sistemico dell'Italia, avvolta tra crisi economica, politica e giudiziaria, ma soprattutto segnata dal male «più grande e più pericoloso: l'odio di sé stessa, quasi la volontà di suicidio»¹⁶. All'inizio degli anni Novanta, l'Iri era il maggior gruppo industriale italiano. Nel 1992, contava oltre mille imprese e 400 mila addetti in numerosi settori, compresi bancario, alimenta-

12. Intervento di B. Grillo all'assemblea degli azionisti di Telecom il 29/4/2010, goo.gl/1mMVuy. La vicenda di Telecom si intreccia anche con la carriera di Gianroberto Casaleggio, che toccò il tema, tra l'altro, nel suo dialogo con Grillo e Dario Fo: «Telecom Italia nel 1999, con la sua cessione a debito, si è fermata, ha avuto un infarto dal quale non si è più ripresa. (...) Il risultato è che tecnici, informatici e ingegneri sono in mezzo a una strada o sono emigrati. Negli ultimi trent'anni abbiamo distrutto un patrimonio, una ricchezza enorme che apparteneva al paese, da Olivetti a Telettra, dall'informatica alle telecomunicazioni, senza che nessun politico abbia mosso un dito» (B. GRILLO, D. FO, G. CASALEGGIO, *Il Grillo canta sempre al tramonto*, Milano 2013, Casaleggio Associati, cap. «Caduta libera dell'Italia: perché?»).

13. Merita una menzione V. COZZOLI, *Un decennio di privatizzazioni: la cessione di Telecom Italia*, Milano 2004, Giuffrè, considerando che l'autore è capo di gabinetto del ministro dello Sviluppo economico Luigi Di Maio.

14. Il documento del 2007 da cui citeremo è consultabile presso il profilo Slideshare di Vito Gamberale goo.gl/EpKruY, da cui si cita nelle note seguenti.

15. F. DE BORTOLI, *Poteri forti (o quasi)*, Milano 2017, La Nave di Teseo, p. 94. Su Marisa Bellisario, alla quale è intitolata la Fondazione omonima per la promozione della professionalità femminile, si veda B. CURLI, «Tecnologie avanzate e nuovi "stili" manageriali. Marisa Bellisario dalla Olivetti alla Italtel», *Annali di Storia dell'Impresa*, 18, 2007, pp. 127-169.

16. L. CAFAGNA, *La grande slavina*, Venezia 2012 (ed. or. 1993), Marsilio, p. 188.

re e molte frattaglie. Nel 2000, rimanevano pochissime attività residue, poi fatte confluire in Fintecna, prima della liquidazione dell'Iri nel 2002. Secondo il calcolo di Ravazzi¹⁷, circa il 40% degli incassi derivanti da dismissioni effettuate in Italia tra il 1992 e il 2002 provenne da società dell'Iri. Tra di esse, la galassia delle telecomunicazioni¹⁸, in cui aveva impresso il suo segno precoce un manager del fascismo e della ricostruzione, Guglielmo Reiss Romoli (1895-1961), che Luigi Einaudi considerò simbolo del «miracolo italiano, miracolo che da sé non accade, se non ci sono gli uomini, grandi o piccoli, i quali lo fanno capitare»¹⁹. Reiss Romoli ebbe una vita avventurosa. Capitano dei granatieri di Sardegna nella prima guerra mondiale, lavorò poi per la Banca Commerciale Italiana, occupandosi di reti (riorganizzazione dell'Italgas). Dal 1932 fu alla Sofindit (Società finanziaria industriale italiana), dove avviò la riorganizzazione delle varie società telefoniche controllate dalla Sip elettrica. Dal 1935 direttore della sede di New York della Comit, all'ingresso dell'Italia in guerra venne internato nella prigione di Ellis Island. Tornato in Italia nel 1942, cercò di arruolarsi in quanto fascista della prim'ora ma fu costretto a vivere in clandestinità in quanto ebreo. Dal 1946 tornò sul terreno delle telecomunicazioni: alla direzione generale di Stet imprese una svolta al settore, anche grazie all'acquisizione della Siemens di Milano dal Comitato internazionale per la liquidazione dei beni tedeschi in Italia²⁰.

Il dinamismo di Reiss Romoli non era sempre compreso dalla classe dirigente italiana. Guido Carli raccontò il peso del conservatorismo sociale di Donato Menichella. Il governatore della Banca d'Italia «non accettava l'idea di un telefono in ogni nucleo familiare, gli sembrava un'inutile avventura consumistica, il telefono serviva soltanto al medico condotto, al farmacista e all'ostetrica, per il resto, se ne era fatto a meno per tanti secoli...». Al contrario, la questione telefonica poteva essere vista in termini geopolitici, seguendo «l'idea cavouriana di un'Italia lunga, montagnosa, da unificare anche e soprattutto attraverso un sistema di reti, e infrastrutture». Le ferrovie stavano a Cavour come le telecomunicazioni a Reiss Romoli²¹.

Nel paesaggio di fine Novecento, l'impulso all'unificazione, volto a costruire opportunità di sviluppo per le imprese e i cittadini italiani, si unì alla questione dell'espansione internazionale. Nel 1994 il consiglio di amministrazione dell'Iri approvò il Piano di riassetto delle telecomunicazioni, che prevedeva la creazione di un gestore unico per i servizi di telecomunicazioni. Il settore venne modulato attraverso i due pilastri del riassetto e della privatizzazione.

17. Si veda *Storia dell'Iri*, volume IV: 1990-2002. *Crisi e privatizzazione*, a cura di R. ARTONI, Roma-Bari 2014, Laterza.

18. Dagli anni Novanta vi sono diverse trasformazioni e adattamenti, ma in questo articolo si userà soprattutto la dizione «Telecom», per identificare quella galassia.

19. L. EINAUDI, «Prediche della domenica», *Corriere della Sera*, 30/4/1961.

20. Si riprende qui la voce «Guglielmo Reiss Romoli» di B. BOTTIGLIERI, in *Protagonisti dell'intervento pubblico*, a cura di A. MORTARA, Milano 1984, Franco Angeli, pp. 722- 772.

21. G. CARLI, *Cinquant'anni di vita italiana*, in collaborazione con P. PELUFFO, Roma-Bari, 1996, Laterza, p. 147. Sull'idea cavouriana, si veda l'editoriale «Proviamo a esistere», *Limes*, «Quanto vale l'Italia», n. 5/2018.

L'espansione estera è una delle caratteristiche di Telecom Italia negli anni Novanta. La società acquista profondità internazionale, muovendosi prima dei competitori, inserendosi nei processi di privatizzazione, partecipando alle gare. Secondo Gamberale, «furono raggiunti, in pochi anni – dal '94 al '98 – risultati impensabili. Mai forse un gruppo industriale italiano era stato in grado di proporsi come protagonista di sviluppo internazionale come lo fu Telecom Italia in quel ristretto periodo». Sotto la guida della squadra manageriale di Ernesto Pascale, la campagna estera della galassia Telecom nel fisso la porta negli Stati Uniti, in Messico, India, Francia, Ecuador, Austria, e soprattutto in Spagna, Argentina, Brasile. I risultati del mobile sono straordinari. «Tim, a fine '98, è il leader della telefonia mobile a livello mondiale: lo è per avanguardia nei servizi, per numero di clienti gestiti nel proprio paese, per diffusione e clienti nel mondo, per efficienza, per capitalizzazione di Borsa, per basso livello di indebitamento (meno di 8 miliardi di euro, verso una capitalizzazione di 37 miliardi di euro)»²². Gamberale ha mostrato come il primato sia rovesciato nella struttura attuale dei ricavi di Telecom rispetto ai principali competitori europei, in grado di diversificarsi maggiormente sui mercati internazionali. Inoltre, negli anni Novanta il Csel (Centro studi e laboratori telecomunicazioni) giocò un ruolo chiave nella ricerca e nello sviluppo a livello internazionale, con la nascita dell'MP3 grazie alla squadra guidata da Leonardo Chiariglione²³.

3. Il 27 ottobre 1997 Telecom Italia, privatizzata, veniva ammessa agli scambi a Piazza Affari. La sua travagliata vicenda rientra nelle debolezze del capitalismo italiano, ma anche nel rapporto con la Commissione europea che ha portato alla firma dell'accordo Andreatta-Van Miert (1993) e al netto ridimensionamento del controllo pubblico dell'economia in Italia²⁴. Al tempo questo passaggio era visto come un obiettivo geopolitico e morale. Da governatore della Banca d'Italia, Draghi commemorò Andreatta ricordandone l'enfasi sulla caduta dell'economia pubblica nel 1989: «Se è caduto il muro di Berlino possono cadere altri steccati. Anche la Banca commerciale italiana, la Stet possono essere privatizzate, e senza che lo Stato detenga percentuali di controllo»²⁵. Né controllo né presidio: negli anni No-

22. V. GAMBERALE, *op. cit.*, p. 21.

23. Chiariglione è noto come «inventore dell'MP3», ma ha ricordato: «Nella maggior parte dei casi c'è qualcuno che rappresenta un lavoro, ma c'è un gruppo di lavoro dietro un progetto. Quello che abbiamo fatto assieme a quel gruppo, di cui ero la guida, ha cambiato la musica: sarebbe antistorico negarlo» (G. SIBILLA, «Leonardo Chiariglione, l'uomo che ha reso liquida la musica», *Wired*, 8/5/2014, goo.gl/Dkd7d2).

24. Nella sua autobiografia, Paolo Savona (al tempo ministro dell'Industria) sostiene che il suo contrasto con Van Miert relativo alla siderurgia aveva portato Ciampi, su iniziativa dello stesso Savona, a considerare la questione un problema di «credibilità del paese», da trattare a livello di politica estera e non nel semplice ambito politico-economico, anche se ciò genera un «accordo di sistema» dal quale Savona si dissocia. Secondo Savona, Andreatta «non si limitò a garantire la serietà degli impegni che intendevamo prendere, ma trattò e firmò un accordo per la chiusura delle partecipazioni statali, qualcosa che la Commissione non chiedeva, né io condividevo, ritenendole strumento di politica economica ancora utile, purché ben gestite» (P. SAVONA, *Come un incubo e come un sogno. Memorialia e Moralia di mezzo secolo di storia*, Soveria Mannelli 2018, Rubbettino, p. 224).

25. B. ANDREATTA riportato da *Italia oggi*, 14/11/1989, *Resoconto della presentazione di Prometeia, Il mercato azionario italiano. Elementi per un confronto internazionale*, Milano 1989, EdE, citato in M. DRAGHI, «Beniamino Andreatta economista», 13/2/2008, p. 8.

vanta lo Stato optò per una privatizzazione totale di Telecom, considerandola un passaggio di credibilità necessario per l'ingresso dell'Italia nell'euro. La proroga dell'accordo Andreatta-Van Miert²⁶ menzionava in modo esplicito gli impegni sulle telecomunicazioni.

Draghi, al tempo direttore generale del Tesoro (1991-2001), era «sospettato dai critici più severi di voler rafforzare la più potente holding pubblica europea e non di essere il regista delle privatizzazioni»²⁷. A suo modo, Draghi creò l'Agence des participations de l'État in Italia (in Francia vedrà la luce solo nel 2004) ma, al contrario dei suoi critici dell'epoca, ne vedeva il ruolo in termini ristretti: non l'État actionnaire, ma la realizzazione del mandato di Carli e Andreatta, con la chiusura dell'economia mista e la costruzione in Italia di un moderno mercato dei capitali, grazie alla nuova legislazione sul tema²⁸.

Non è questa la sede per affrontare il nodo del rapporto tra liberalizzazioni e privatizzazioni. Nel caso di Telecom, oltre alla privatizzazione in sé, bisogna considerare il lavoro che l'ha preceduta, che si intersecò con un elemento decisivo: i successi del management, soprattutto relativi alla telefonia mobile, grazie tra l'altro alla prima carta telefonica prepagata e ricaricabile per la rete Gsm, Tim card. La grande controversia non riguarda la fusione tra Stet e Telecom che, secondo Scannapieco, «ha creato valore in quanto ha permesso di ridurre i costi, razionalizzando le strutture gestionali, cioè eliminando le sovrapposizioni organizzative»²⁹. La storica polemica coinvolge gli assetti proprietari della privatizzazione. Nel collocare in Borsa Telecom, il Tesoro volle costituire un insieme di azionisti in grado di garantire la stabilità dell'azienda. Il nocciolo duro si trasformò in «nocciolino», garantito dalla principale famiglia industriale italiana, gli Agnelli. Il nocciolino deteneva il 6,7% della compagnia telefonica. Decisivo lo 0,6% di Ifil della famiglia Agnelli, perché il resto del nocciolino era disperso tra azionisti del risparmio, delle banche e delle assicurazioni³⁰. Al nocciolino corrispondeva un conflittino, anzi «un conflitto minimo, il più piccolo che si possa immaginare». Così si esprime lo stesso Giovanni Agnelli all'uscita dal Senato, rispondendo a Cossiga il quale aveva criticato come, con quella proprietà, fosse possibile controllare di fatto «quello che fino a ieri è stato patrimonio di tutti gli italiani»³¹. Una buona sintesi sullo stato di Telecom fu fornita da un protagonista successivo: «Non è più dello Stato, ma non si capisce bene di chi sia»³².

26. Disponibile ancora sul sito della Commissione europea goo.gl/rNjp2e

27. Così *la Repubblica*, 18/10/1997.

28. Sul ruolo e la salvaguardia dei piccoli azionisti in questo sistema, essenziale l'aspra polemica tra Mario Draghi e Guido Rossi, che se le diedero di santa ragione su *la Repubblica* nel 2001.

29. D. SCANNAPIECO, «Le privatizzazioni in Italia: una riflessione a dieci anni dal rapporto presentato al ministro del Tesoro Guido Carli», in *Guido Carli e le privatizzazioni dieci anni dopo*, a cura di F.A. GRASSINI, Roma 2001, Luiss Edizioni, pp. 178-179.

30. *Libro bianco sulle privatizzazioni*, ministero del Tesoro, del bilancio e della programmazione economica, aprile 2001, p. 51.

31. *Archivio AdnKronos*, 27/10/1998, goo.gl/E4y3J5

32. «Telecom? Lasciamoli lavorare», *la Repubblica*, 22/4/1998. «Lasciamoli lavorare» è una frase infelice di Umberto Agnelli sul management della Telecom dell'epoca.

La stabilità dell'azienda, che perse Pascale e parte della sua squadra, non fu mai raggiunta. Non nella stagione italiana, attraverso le operazioni di Borsa che hanno visto protagonisti Colaninno e Gnutti (1999), poi Tronchetti Provera e i Benetton (2001). I protagonisti italiani sono stati avvolti nella polemica di Telecom, in particolare sul debito che grava sul gruppo, sulle gestioni immobiliari, sulla banda larga. Hanno fornito la loro versione dei fatti nei bilanci, nelle testimonianze personali e degli storici. Il giudizio dipende, oltre che dai numeri e dalle strategie, dal peso che si dà allo status di Telecom come «la camera di compensazione silenziosa e il luogo di regolazione dei conflitti più duri, tra economia e politica»³³. Nell'ottica della geopolitica dell'Italia, resta un fatto: in anni successivi, Colaninno e Tronchetti Provera hanno colto opportunità internazionali di prim'ordine per Piaggio e Pirelli, guardando all'Asia. Il profilo internazionale del gruppo delle telecomunicazioni si è invece indebolito.

La stabilità non giunse coi soci industriali stranieri, prima spagnoli (2007) e poi francesi (2015), che non hanno mai trovato un *modus vivendi* con l'Italia. Anche qui la vicenda Telecom ha mostrato un segno geopolitico: la ferita delle illusioni europee. In particolare, l'illusione che, nelle telecomunicazioni, sarebbero nati ben presto giganti europei (una «Airbus delle telecomunicazioni»), per pesare in nuove creature gli assetti proprietari nazionali. L'eurocrate per eccellenza, Martin Selmayr³⁴, dichiarò perentorio nel 2007: «La nazionalità delle imprese non deve avere alcun ruolo sul mercato»³⁵. Difficile capire se Selmayr ci credesse e ci creda davvero, ma quello che conta è la realtà: gli Stati europei non si sono mai adeguati a tale principio. L'Italia ha percorso la strada più confusa: la vendita totale dell'azienda, quindi la smobilitazione del presidio e del vincolo dello Stato, che non rimosse la discrezionalità politica nella sua vita, intersecandosi con la vicenda di una *golden share* prima presente, poi abbandonata, poi tornata in altre forme. Germania e Francia hanno evitato questa telenovela, con la partecipazione diretta in Deutsche Telekom del governo tedesco e di KfW, con le quote del governo francese e di Bpifrance Participations in Orange. In Spagna, il nucleo della privatizzazione era vero, garantito dall'ampia quota detenuta dalle banche e dai poteri statuali su Telefónica. La letteratura accademica ricorda che lo Stato spagnolo «influenzò la sua struttura proprietaria durante il processo di privatizzazioni, protesse la posizione dominante di Telefónica nel mercato interno, selezionò le principali figure manageriali di Telefónica e ne supportò l'espansione estera»³⁶. Il problema non sta dunque nel ruolo dello Stato per sé. La differenza è che tale ruolo in Italia nella vicenda Telecom è stato confuso, occasionale, privo di certezze.

33. P. BRICCO, «Telecom e il potere, quell'intreccio lungo un secolo», *Il Sole-24 Ore*, 5/5/2018. Queste vicende, come quelle giudiziarie, non possono essere affrontate pienamente in questa sede, dovendosi dare priorità agli aspetti geopolitici.

34. Al tempo portavoce del commissario per i Media e la società dell'informazione, ora segretario generale della Commissione europea.

35. Dichiarazione riportata dal *Corriere del Sera*, 18/4/2007, goo.gl/fLfSrr.

36. F. BULFONE, «The State Strikes Back: Industrial Policy, Regulatory Power and the Divergent Performance of Telefónica and Telecom Italia», *Journal of European Public Policy*, 2018, p. 4.

Nella sua lettura dei fatti, la squadra di Draghi ha sottolineato il legame tra la liberalizzazione dei mercati e la rimozione dei poteri speciali dovuti alla quota dello Stato, che aveva portato alla condanna dell'Italia da parte della Corte di giustizia europea. Eppure, la posizione ideologica dell'inizio degli anni Duemila, per cui i poteri speciali fossero opportuni da ultimo solo in Finmeccanica, appare oggi limitata, perché risente di un concetto ingenuo di «difesa» e di «sicurezza nazionale». O meglio, si tratta di una concezione che risponde a criteri economici, mentre nell'attuale scenario sono più evidenti i criteri geopolitici³⁷.

4. «Vengono, inoltre, in sempre maggiore evidenza i profili di sicurezza relativi al settore delle comunicazioni, oggetto di un intenso processo di innovazione tecnologica»³⁸. Così l'allora vicepresidente del Consiglio dei ministri Sergio Mattarella, nel suo saluto all'inaugurazione dell'anno accademico 1999/2000 della Scuola di addestramento del Sisde. Quasi vent'anni dopo,

il profilo di sicurezza trovò la sua intersezione con la storia infinita di Telecom. Con un antecedente: la lunga campagna di Vincent Bolloré in Italia, che cominciò all'inizio degli anni Duemila grazie al suo coinvolgimento in Mediobanca. Dopo l'uscita di Vincenzo Maranghi nel 2003, Bolloré divenne il punto di riferimento del nucleo francese di Piazzetta Cuccia (un nucleo vero, erede della linea Cuccia-Meyer), che al tempo comprendeva anche Dassault e Groupama. Da quel momento Bolloré

SVILUPPO DI TELECOM ITALIA ALL'ESTERO, SU RETE FISSA

1994

Impsat Corporation, Delaware Usa

1995

Citel Corporación interamericana de telecomunicaciones - Messico

1996

Impsat e Norcable - Argentina

Bharti Tele-Ventures - India

Stet France

1997

9 Télécom - Francia

Intelcom San Marino

Euskaltel, Cyc Telecomunicaciones, Netco Redes, Retevisión e Cable Televisivo de Catalunya - Spagna

Telecom Serbia

Nethetelec - Ecuador

1998

Multimedia cable - Spagna

*Solpart Participações - Brasile
(holding di controllo di Brazil Telecom)*

Telecom Austria

1999

Nortel Inversora - Argentina

Auna - Spagna

BB Ned - Paesi Bassi

Med 1 Submarine Cable Mediterranean Broadband Access - Grecia

Mediterranean Nautilus - Irlanda

37. Si confronti D. SCANNAPIECO, *op. cit.*, p. 184, con A. ARESU, in questo volume.

38. L'intervento, che conserva un'importanza anche per l'attenzione alla disciplina normativa dei servizi, si può leggere all'indirizzo goo.gl/1uPpCL. Per gli amanti delle «coincidenze significative», dopo l'intervento di Mattarella è riportato quello di Paolo Savona.

giocò un ruolo importante nel nodo Mediobanca-Generali. Il 2002 fu l'anno del ritorno al vertice del Leone di Trieste di Antoine Bernheim, il «padrino del capitalismo francese»³⁹ che dei suoi pupilli Arnault e Bolloré disse «*C'est moi qui les ai faits*» («sono io ad averli creati»). Poi accusò Bolloré di averlo abbandonato nel 2010, supportando l'ascesa di Geronzi a Trieste.

L'uscita di Telefónica dall'azionariato di Telecom, a seguito dei problemi di antitrust in Sudamerica, fornì un'opportunità a Bolloré, che con Vivendi tra il 2015 e il 2016 divenne il maggiore azionista della società. Nel mentre, Vivendi portò avanti una trattativa per l'acquisizione di Mediaset Premium, per poi ritirarsi e puntare direttamente a Mediaset. Sembrò che Bolloré volesse realizzare il «piano Rovati» a modo suo, con la variante dell'ingresso in Italia dell'Iliad di Xavier Niel, anch'egli tra il 2015 e il 2016 affacciandosi in Telecom. Il cuore delle telecomunicazioni italiane si sentì «in una di queste scorriere sopraffatto da' Francesi»⁴⁰. L'operazione si accomodò in un grande calderone: la Libia, la difesa, la finanza. Sotto la pelle del conflitto italo-francese rimase la paura che, dopo l'acquisizione del gigante del risparmio gestito Pioneer da parte di Amundi, potesse realizzarsi la profezia di Maranghi: la conquista di Generali da parte dei francesi di Axa. Magari per testare il principio di Selmayr sul ruolo inesistente della nazionalità su un tema sensibile: il sostegno al debito pubblico italiano.

Alla fine del 2015, sotto gli auspici del governo allora guidato da Matteo Renzi, nacque Open Fiber, società di Enel volta a realizzare una rete a banda larga diffusa ed efficiente. La società, che nel 2016 divenne partecipata alla pari dal gruppo Cassa depositi e prestiti ed Enel, dichiarò l'obiettivo ambizioso di raggiungere entro il 2020 oltre 10 milioni di utenze, aggiudicandosi nel 2017 i primi bandi Infratel. La concorrenza per Telecom rappresentò uno stimolo, segno della vitalità della società. Riccardo Ruggeri, il grande manager di New Holland, l'ha sintetizzata con un tweet caustico: «Telecom? La carcassa di un elefante che da anni alimenta, sempre con carne fresca, diversi animali della savana»⁴¹. Appunto, carne fresca. Non frollata. Resistono competenze di lungo corso nella forza lavoro. Nei momenti in cui l'azienda si trova sfidata sul mercato, riesce a reagire.

Resta una questione aperta, che non può essere valutata in termini di mercato: l'aspetto di sicurezza di alcuni asset. Tema già emerso – con ritardo – nel 2013⁴², davanti alle mire di Telefónica. Nel governo Monti la *golden share*, colpita da Bruxelles, venne ripensata da un esperto dei processi europei, Enzo Moavero Milanesi, legando i poteri ai settori strategici per il paese e non al possesso delle azioni. Non senza affanni attuativi e di impulso politico, la disciplina dei poteri speciali, seguendo una tendenza di «geopolitica della protezione» che caratterizza in primis gli Stati Uniti, è stata poi approfondita. Tre impulsi princi-

39. Riprendo P. DE GASQUET, *Le parrain du capitalisme français*, Paris 2010, Grasset.

40. Così gli *Annali d'Italia* di L.A. MURATORI (1743-1749). Devo a Sara Rossi il suggerimento sulle «scorriere» in Muratori.

41. R. RUGGERI, «Se Cattaneo ha servito con fedeltà il "re" 25 milioni di buonuscita sono pochi», *La Verità*, 26/7/2018.

42. Si veda sul tema la sintesi di A. GIANNULI, *Classe dirigente*, Firenze 2017, Ponte alle Grazie, p. 153.

pali hanno caratterizzato questo processo nel 2017⁴³: l'attenzione dell'intelligence, il dinamismo dell'allora ministro dello Sviluppo economico Carlo Calenda, la perizia del vicesegretario generale della presidenza del Consiglio, Luigi Fiorentino, incaricato della questione dal punto di vista amministrativo poiché alla guida del Gruppo di coordinamento interministeriale per i poteri speciali, ai sensi dell'art. 3 del dpcm del 6 agosto 2014. In particolare, il dpcm del 16 ottobre 2017, pochi giorni dopo la lettera degli ex manager di Telecom che ripropone l'idea «carsica» dell'ingresso di Cassa depositi e prestiti nel capitale⁴⁴, è frutto di questo processo. Vi si afferma che la società di telecomunicazioni «direttamente o indirettamente mediante le sue controllate detiene asset e svolge attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale», superando le precedenti sottovalutazioni del tema. Il decreto, nello stabilire precisi controlli organizzativi relativi alla sicurezza e assegnando un ruolo ai servizi, menziona in particolare Telecom Italia Sparkle e Telsy. Telsy è una piccola ma significativa società che fornisce apparati di sicurezza: durante l'ennesimo interregno di Telecom, nel 2014, si poteva visitare la mostra «Crypto» presso il Museo tecnico navale della Spezia e visionare alcuni dei dispositivi di crittografia della sua storia, come Telsy TDS-2003, Telsy TDS-2004, Telsy TDS-2004M, esposti accanto a Enigma. Difficile sottovalutare l'importanza di Sparkle⁴⁵. Anche i suoi natali (col nome Telemedia International Italia) rimandano a Pascale, alla guida di Italcable al tempo della sua creazione nel 1987. Sparkle ha fatturato 1,4 miliardi di euro nel 2016, ha una importante estensione fisica, con una dorsale globale di circa 560 mila chilometri di fibra e cavi sottomarini internazionali⁴⁶, da cui passa tra l'altro l'80% del traffico voce e dati dal Mediterraneo all'America⁴⁷. I suoi *data centers* si trovano a Palermo, ad Atene (Metamorphosis e Karopi), a Istanbul e a Miami.

Il prosieguo del 2018 ha visto una caduta delle fortune di Bolloré, fermato su Mediaset, che raggiunge a marzo un accordo di collaborazione con Sky Italia⁴⁸. Nel 2018 Rovati, morto nel 2013, ha vinto la sua scommessa, con l'ingresso di Cassa depositi e prestiti nel capitale di Telecom in una prospettiva di lungo periodo, per una quota non superiore al 5%⁴⁹. L'intervento di Cassa depositi e prestiti avviene nell'aprile 2018, all'indomani delle elezioni. Momento di instabilità che richiede l'impulso di ciò che è stabile (le fondazioni bancarie⁵⁰) e l'ampio consenso delle

43. Nel governo di Paolo Gentiloni, che era stato ministro delle Telecomunicazioni nei passaggi del 2006-8 della storia di Telecom.

44. F. CHIRICHIGNO, U. DE JULIO, G. DI GENOVA, V. GAMBERALE, «Gli ex vertici: Telecom è strategica, lo Stato rientri nel capitale», *Corriere della Sera*, 25/9/2017, goo.gl/1t9BRX

45. L'amministratore delegato e direttore generale di Open Fiber dal gennaio 2018, Elisabetta Ripa, è stata amministratore delegato di Telecom Sparkle.

46. www.tisparkle.com/our-assets/global-backbone.

47. A. OLIVIERI, «Telecom Sparkle, che cosa nasconde la rete di cavi che fece gola ad AT&T», *Il Sole-24 Ore*, 4/8/2007.

48. Comunicato Mediaset del 30/3/2018, goo.gl/b4D7FG.

49. «CDP: il Cda delibera l'ingresso, con una prospettiva di lungo periodo, nel capitale di Telecom Italia S.p.A. (TIM)», 5/4/2018, goo.gl/fBP6Sk

50. L'attenzione del presidente dell'Acri Giuseppe Guzzetti è menzionata dalla giornalista più informata sulle fondazioni bancarie, Camilla Conti, e da Paolo Bricco. Tra gli interventi di Guzzetti su Telecom, memorabile il suo rifugio nel dialetto milanese, invitando nel 2015 di evitare la sindrome

forze politiche, implicito ed esplicito. Giancarlo Giorgetti della Lega parla di «finalità giusta, condivisa in termini politici»⁵¹. Roberta Lombardi del Movimento 5 Stelle twitta «Cassa depositi e prestiti nel capitale #TIM a difesa della rete, un asset strategico per il paese»⁵².

Nel maggio 2018, Cassa depositi e prestiti supporta la lista per il Consiglio di amministrazione presentata dal fondo attivista Elliott di Paul Singer, che in una sfida che coinvolge anche gli investitori istituzionali (poco rispondente alla dottrina Selmayr) batte di misura la lista di Vivendi. Arriva alla presidenza Fulvio Conti, già in Telecom alla fine degli anni Novanta e artefice dell'espansione internazionale di Enel, fallita in Francia per la linea di difesa del governo, riuscita in Spagna e quindi in Sudamerica. Con Elliott ritorna la «questione americana», che nel gruppo delle telecomunicazioni si è incarnata soprattutto nei rapporti con At&t in due momenti storici. Il primo a cavallo della privatizzazione, quando l'ingresso di At&t nel capitale (fuori dal nocciolino) fu il preludio di un'alleanza mai andata in porto. Il secondo si intersecò con il piano Rovati e con le reazioni degli operatori tradizionali delle telecomunicazioni all'avanzata di Google e Yahoo, che per lo storico manager texano di At&t Edward Whitacre Jr. dovevano pagare gli investimenti in infrastrutture e non potevano pretendere di usare gratis i tubi⁵³. Il ritiro della proposta di investimento di At&t su Telecom nel 2007 portò a un duro e controverso intervento pubblico, sul *Corriere della Sera*, dell'allora ambasciatore degli Stati Uniti in Italia, Ronald Spogli, che vi colse la cartina di tornasole dell'incapacità italiana di attrarre investimenti⁵⁴.

5. Molte sono le incognite sul futuro dell'azienda, in uno scenario ideologico molto diverso da quello degli anni Novanta. Non c'è più il vento in poppa per la «leggenda nera» dell'Iri, alimentata dalla battuta sui «panettoni di Stato». Forse è giunto il momento di dire che i manager dell'Iri non hanno mai voluto fare panettoni. Sono stati i politici a imporre loro di salvare aziende alimentari. All'autonomia manageriale dell'Iri non è stato sostituito nulla. Nessuno in Italia ha investito in modo adeguato in ricerca, né il pubblico né il privato. Una proposta coraggiosa come quella di Assolombarda del 2018, istituire con 10 miliardi di euro «un Fraunhofer italiano della ricerca per l'industria e la manifattura, sullo stesso modello del 30% di finanziamento pubblico e del 70% a carico delle im-

del «padron de la melonera», il venditore di meloni che si sbraccia con prepotenza per imporre i suoi prodotti. Si veda goo.gl/i8fE55

51. M. ZACCHE', «Cdp-Tim, applaudono tutti tranne la lobby finanziaria Pd», *Il Giornale*, 9/4/2018, goo.gl/LUn5NC

52. Tweet di Roberta Lombardi, 8/4/2018. Il 19 luglio 2017 si sono svolte le votazioni su Rousseau relative al Programma telecomunicazioni del Movimento 5 Stelle, in cui 16.275 votanti su 17.463 hanno sostenuto che per lo sviluppo della banda larga l'infrastruttura di rete deve essere pubblica e gestita da una società pubblica, goo.gl/aXFdmu

53. La sua celebre dichiarazione del 2005 fu: «They don't have any fiber out there. They don't have any wires. They don't have anything. They use my lines for free – and that's bull. For a Google or a Yahoo! or a Vonage or anybody to expect to use these pipes for free is nuts!» («The Origins of the Net Neutrality Debate», *MIT Technology Review*, 8/7/2006).

54. R.P. SPOGLI, «L'Italia e gli investimenti che non arrivano», *Corriere della Sera*, 19/4/2007, goo.gl/1xoGwL.

prese»⁵⁵, doveva essere realizzata all'inizio del secolo. Ora è comunque necessaria, ma sarà di difficile attuazione. Rimane in Telecom una notevole capacità di ricerca e sviluppo industriale: lo *R&D Investment Scoreboard* 2017 della Commissione europea pone Telecom con 1,748 miliardi al settantottesimo posto al mondo, prima delle aziende italiane e in grado, con Leonardo, di contare per il 52% degli investimenti italiani⁵⁶.

Quindi, che cosa dobbiamo fare? La storia delle privatizzazioni sarà riscritta⁵⁷, e continuerà a essere terreno di scontro, mentre potrebbe essere occasione di riconciliazione con gli errori per allargare la prospettiva storica, imparando gli uni dagli altri. Chi oggi elogia il ruolo dello Stato dovrà sempre ricordare il monito di Ernesto Rossi, nel cuore della ricostruzione: «Queste collettivizzazioni e questo intervento non significano un aumento di autorità dello Stato, né si svolgono secondo un piano unitario, nell'interesse dell'intera collettività nazionale; corrispondono invece ad una progressiva dissoluzione dello Stato in feudi governati da alcuni gruppi industriali e da alcune piccole camarille di funzionari, che si combattono, si alleano, si collegano fra loro, nel loro esclusivo interesse»⁵⁸. Una campana che suona ancora, soprattutto per il capitalismo municipale. Inoltre, in Italia permane un senso equivoco della sicurezza, pericoloso quanto la sottovalutazione dei profili di sicurezza delle telecomunicazioni. Lo Stato deve occuparsi forse di sicurezza alimentare comprando le aziende alimentari? Deve occuparsi di sicurezza occupazionale gestendo direttamente le industrie? No. Sia perché non ci sono i soldi sia perché, se tutto è sicurezza, niente è sicurezza. Sparkle è sicurezza, gli alberghi non lo sono. E l'ordinamento italiano dovrebbe riconoscerlo con chiarezza.

Il destino di Telecom resta incerto, anche in ottica geopolitica. Lambisce il conflitto tra Italia e Francia, che richiede la chiusura di alcuni dei suoi troppi fronti. È inutile che i due paesi si definiscano «nemici», che Salvini e Macron si riconoscano quali comodi avversari, magari per poi ritrovarsi incapaci entrambi di costruire vere alleanze con altri. È inutile soprattutto per l'Italia, che non è nelle condizioni di recuperare nel breve periodo il ritardo verso la Francia nell'intelligence economica e nella difesa, tantomeno tagliando la difesa. Ormai sarebbe più proficua – nonché più divertente – una schietta ripresa dei dialoghi sul Trattato del Quirinale con una sezione introduttiva in streaming, dove la parte italiana potrebbe cooptare Giulio Sapelli come capo delegazione. L'altro fronte concerne le vie della seta digitali. Rovati parlava della «Terna delle telecomunicazioni»: forse potrebbe affacciarsi un destino simile a quella del resto di Terna, con la Cina in Cdp Reti, su cui il governo nel 2014 decise di non applicare le prescrizioni dei poteri speciali.

55. C. BONOMI, «La responsabilità del futuro», Assemblea generale di Assolombarda, Milano, 18/10/2018, p. 20.

56. Dati presenti nel sito iri.jrc.ec.europa.eu/scoreboard17.html. Questa sezione della Commissione europea è dedicata a «Economics of Industrial Research and Innovation». Perciò, alla destra del logo della Commissione, chi naviga nel sito può leggere: Iri.

57. Significativa a questo proposito la serie di *La Verità* sulle privatizzazioni, e in particolare C. CAMBI, «Così i predoni rossi si papparoni Telecom», *La Verità*, 31/8/2018, di grande interesse per i virgolettati di Ernesto Pascale.

Ma i futuri sviluppi delle telecomunicazioni non avverranno senza una maggiore attenzione degli Stati Uniti, perché la guerra fredda tecnologica con la Cina è in corso e mette un peso geopolitico sulle varie aste internazionali del 5G. Le contromosse di Pechino arriveranno. Ciò non deve però portare a una sopravvalutazione dell'investimento strategico di Washington sulle questioni italiane, considerando Elliott come proxy immediato dell'amministrazione Trump, con Singer impegnato a tempo pieno a ridisegnare l'intero governo del capitalismo italiano, da Mediobanca a Generali, con capitali illimitati⁵⁹. Le cose non stanno così: da un lato, Elliott è un partner finanziario, non industriale, anche se capace di attrarre una rete di storici manager italiani. Pertanto, Elliott, che ha anche altro da fare, considera i rendimenti, e tiene senz'altro presenti le difficoltà del titolo, che riguardano tutti, soprattutto in uno scenario di turbolenza dei mercati. Aleggia ancora la questione Mediaset. Allargando lo sguardo, fuori ci sono le trasformazioni delle telecomunicazioni, dove le infrastrutture fisiche continuano ad avere un peso, mentre i giganti digitali continuano la loro corsa.

Se l'Italia si fissa nello specchio di Telecom, formula domande sul passato, con la musicalità del congiuntivo telefonico: e se Pascale fosse rimasto? Se il governo avesse mantenuto una quota? Se a un gruppo Iri razionalizzato fosse stata consentita l'opzione percorsa con l'Eni? Se la public company iniziale fosse stata vera? Se la separazione dell'infrastruttura fosse giunta prima della privatizzazione? Se il mercato degli investitori istituzionali italiani fosse stato più maturo? Se la classe manageriale degli Agnelli di fine anni Novanta fosse già passata per la cura Marchionne? Se manager e lavoratori Telecom avessero preso una quota? Innumerevoli «se», in un passato che non può tornare e a cui non si può dire addio. Non si può vivere di rimpianti, ma l'autobiografia di un paese si fa anche attraverso i se, per maturare e acquistare profondità storica. Per afferrare le sfide di oggi, che riguardano Telecom e l'Italia, avvolgono i suoi cavi e i suoi doppi, fisici e mentali: rilanciare la ricerca, definire la sicurezza, limitare la confusione.

58. E. Rossi, «Attenti alle mosche», *Il Mondo*, 30/6/1951, in *Il Malgoverno*, Bari 1954, Laterza, p. 124.

59. Anche se le mosse di Elliott meritano di essere analizzate, come fa S. CINGOLANI, «Non solo Bonucci-Higuain: il futuro del capitalismo italiano si gioca sull'asse tra Elliott e Exor», *Linkiesta*, 2/8/2018, goo.gl/zQ8iiC. Elliott gestiva 35 miliardi di dollari di asset al 1° luglio 2018 secondo il sito ufficiale www.elliottmgmt.com/about-elliott

LA VIA FRANCESE ALLA SOVRANITÀ DIGITALE

di Francesco MASELLI

Le preoccupazioni di Parigi per attacchi informatici dall'estero si traducono in atti concreti per la tutela dello Stato e del cittadino. Burocrati e militari reggono il passo. I furti cinesi e l'incontrastato dominio americano. Ogni utente però deve fare la sua parte.

1.  POCHE SETTIMANE DALLE ELEZIONI presidenziali del 2017, il ministero degli Esteri francese comunicò ai cittadini residenti all'estero che il sistema di voto elettronico, inizialmente previsto, non sarebbe stato utilizzato per ragioni di sicurezza. In particolare, la comunicazione del ministero motivava la decisione «sulla base delle raccomandazioni degli esperti dell'Agenzia nazionale della sicurezza dei sistemi informatici a causa delle minacce estremamente elevate di ciberattacchi che potrebbero non consentire il corretto svolgimento del voto elettronico». Il governo era preoccupato da eventuali attacchi informatici, anche a causa dell'esperienza vissuta durante le elezioni americane dell'anno precedente, vero bersaglio della propaganda informatica e degli attacchi via Internet, soprattutto da parte della Russia.

L'esempio era ancora abbastanza vivo all'inizio della campagna elettorale del 2017, cominciata proprio a ridosso del voto americano, come dimostrano molte dichiarazioni da parte dei più alti esponenti del governo di Manuel Valls. L'allora ministro degli Esteri, Jean Yves Le Drian, abituato a commenti sobri sui fatti di sua competenza, riassunse invece in modo abbastanza esplicito la situazione durante il Forum internazionale della cbersicurezza a Lille, il 25 gennaio 2017: «Non bisogna abbassare la guardia, la minaccia è alle nostre porte». Seguito dal ministro dell'Interno, Bruno Le Roux, intervenuto nella stessa occasione: «Gli Stati stranieri si mostrano sempre più inventivi (...) i nostri sistemi informatici sono nel mirino di molti attacchi, alcuni mirati, tali da minacciare la nostra sovranità»¹.

2. Il 14 febbraio 2017 un attacco particolarmente intenso al sito di En Marche!, il movimento dell'allora candidato Emmanuel Macron, rese inaccessibile la piatta-

1. Entrambe le dichiarazioni in M. UNTERSINGER, «Cybersécurité: pour Jean-Yves Le Drian, "la menace est à nos portes"», *Le Monde*, 25/1/2017.

forma per alcune ore, e il suo segretario generale, Richard Ferrand, denunciò dalle colonne di *Le Monde* «migliaia di attacchi informatici mensili» che «provengono dall'Ucraina»². Nel mirino, più o meno implicitamente, le attività degli hacker russi, sospettati di parteggiare per la candidata del Front national, Marine Le Pen, e di volere intervenire massicciamente per influenzare l'esito del voto. Ci fosse o meno una regia da parte di Mosca, la Francia aveva già cominciato a prendere delle contromisure, soprattutto nella formazione e nella tutela di tutti i candidati. Nell'ottobre del 2016, secondo le informazioni raccolte dal settimanale *Le Canard enchaîné*³, tutti i candidati a quel punto sicuri di partecipare alle elezioni presidenziali dell'anno successivo furono convocati dal Secrétariat général de la défense et de la sécurité nationale per essere messi al corrente dei rischi che avrebbero dovuto affrontare durante la campagna elettorale.

La riunione, tenuta segreta per mesi e disertata dal Front national, dà l'idea dell'attenzione riservata dall'esecutivo al problema, così come lo dimostra l'allargamento delle attribuzioni della Commission nationale de contrôle de la campagne électorale (Cnccep), l'autorità solitamente incaricata del controllo amministrativo del buon andamento della campagna elettorale. La Cnccep fu infatti incaricata di vigilare anche sul suo svolgimento digitale, con particolare attenzione, appunto, alle attività di disinformazione e hackeraggio messe in campo da potenze straniere, e al supporto dei candidati⁴. Il governo francese organizzò, tra le altre cose, numerosi seminari condotti dall'Agence nationale de la sécurité des systèmes d'information, che si concentrò in particolare sulla formazione dei candidati e dei loro assistenti nell'ambito dell'igiene digitale.

Per rispondere alle nuove minacce, e grazie al contributo formativo dello Stato, tutti i comitati elettorali si dotarono di squadre apposite, incaricate di evitare le infiltrazioni informatiche o di limitare gli eventuali danni. Un'attività condotta con un certo successo soprattutto dal comitato di Emmanuel Macron che, vittima di un attacco massiccio il weekend prima del secondo turno, riuscì a depistare gli hacker con la tecnica del *cyber-blurring*, inserendo cioè nei server moltissime informazioni false indistinguibili da quelle vere⁵. La strategia ha reso impossibile per chi volesse consultare i «Macron Leaks» capire quali informazioni fossero affidabili e quindi utilizzabili per nuocere al candidato, a quel punto diventato presidente, e quali invece no.

3. Il governo francese ha preso molto seriamente la sua funzione di tutela della cosiddetta «sovranità digitale», cioè la necessità di proteggere le attribuzioni dello Stato anche in campi immateriali, che se compromessi immateriali non sono. D'altronde lo stesso ministro Le Drian, in occasione della conferenza di Lille poc'an-

2. R. FERRAND, «Ne laissons pas la Russie déstabiliser la présidentielle en France!», *Le Monde*, 14/2/2017.
3. *Le Canard enchaîné*, 8/2/2017.

4. I. TRIPPENBACH, «Cyberattaques: la Commission de contrôle de la campagne présidentielle veillera», *l'Opinion*, 27/2/2017.

5. A. NOSSITER, D. SANGER, N. PERLROTH, «Hackers Came, but the French Were Prepared», *The New York Times*, 9/5/2017.

zi citata, spiegò con chiarezza che la Francia non considera l'ambiente digitale come astratto o diverso da quelli tradizionali, anche e soprattutto in materia di guerra: «Se un'azione digitale armata utilizzata contro nostri interessi causa una paralisi o dei danni, o ancora una perdita di vite umane, la ritorsione non sarà necessariamente *cyber*. Potremmo», spiega il ministro, «qualificarla come un'aggressione ai sensi dell'articolo 51».

E in effetti già nel 2014 i francesi vararono, all'interno del decreto «sul patriottismo economico», una modifica al codice monetario e finanziario per sottomettere gli investimenti stranieri a un'autorizzazione preventiva quando questi intervengono nelle materie di sicurezza delle reti o nei servizi di comunicazione elettronica⁶. Secondo l'avvocato Eric Caprioli, membro del Club des experts de la sécurité de l'information et du numérique, è significativa anche la nota d'informazione del 5 aprile 2016 inviata dalla Direzione delle collettività territoriali e del Servizio interministeriale degli archivi di Francia, che impone agli uffici della funzione pubblica che intendono avvalersi di sistemi *cloud* per archiviare i loro dati di rivolgersi a fornitori sovrani. L'atteggiamento è rilevante perché implica un'attenzione al dettaglio non scontata per un'amministrazione burocratizzata e ritenuta spesso troppo lenta a percepire i cambiamenti come quella francese⁷.

Allo stesso tempo, numerosi osservatori hanno notato che la forma centralizzata dello Stato francese può tuttavia rivelarsi molto utile per organizzare risposte coordinate e coerenti rispetto alle minacce esterne, in un ambiente dove ridurre gli obiettivi da difendere è di sicuro un importante vantaggio⁸.

L'esercito ha, infine, dedicato uno sforzo intellettuale rilevante alla comprensione delle minacce e delle opportunità che rappresenta il ciberspazio per le operazioni militari, dedicando all'argomento grande spazio nella *Revue stratégique de défense et sécurité nationale* pubblicata nel dicembre 2017, un lavoro condotto dal ministero delle Forze armate per preparare la successiva legge di programmazione militare 2019-25. La legge prevede una disposizione interessante che mostra la volontà di rendere più efficienti le difese dalle intrusioni esterne. L'articolo 19, infatti, in caso di sospetto di attacco imminente contro le autorità pubbliche o contro operatori di telecomunicazione di importanza vitale (Oiv), autorizza l'Agence nationale de la sécurité des systèmes d'information (Anssi) a installare dei sistemi di individuazione delle minacce direttamente nelle sedi di tali operatori, al fine di raccogliere informazioni e prevenire il futuro attacco⁹. I dati potranno essere tra l'altro conservati dall'agenzia per cinque anni prima di essere distrutti, fermo restando il controllo dell'Autorité de régulation des communications électroniques et des postes (Arcep) sul corretto svolgimento delle attività dell'agenzia.

6. Si tratta dell'articolo R153-2.

7. E. CAPRIOLI, «Souveraineté numérique et les enjeux des plateformes de Bug Bounty européennes», *L'Usine Digitale*, 12/02/2018.

8. J. EYAL, «How France Fought off Influence Ops in the Last Election», *The Straits Times*, 2/7/2018.

9. Si veda l'articolo 19 della legge 607/2018 relativa alla programmazione militare per gli anni dal 2019 al 2025, con diverse disposizioni riguardo alla Difesa.

4. L'attenzione non si ferma soltanto alla prassi quotidiana della pubblica amministrazione, ma è alta anche dal punto di vista simbolico e diplomatico. Lo dimostra la carriera di David Martinon, nominato rappresentante speciale della Francia per le negoziazioni internazionali sulla società dell'informazione e dell'economia digitale da François Hollande nel 2013, e successivamente promosso al rango di ambasciatore per la ciberdiplomazia e l'economia digitale, attribuzione che naturalmente ingloba anche i problemi di sicurezza digitale. La Francia non ha tuttavia seguito la strada della Danimarca, che aveva creato un posto simile nel marzo 2017 compiendo un passo ulteriore: il suo ambasciatore è stato infatti accreditato presso i cosiddetti Gafa, Google, Amazon, Facebook e Apple, elevati dunque al rango di Stati con cui trattare anche diplomaticamente.

Un approccio inconcepibile per il Quai d'Orsay, che ha preferito un ruolo meno vistoso e soprattutto flessibile, e ha evitato di limitare l'azione del suo agente diplomatico a una sola area geografica. Martinon, confermato al suo posto da Emmanuel Macron prima di essere poi nominato ambasciatore in Afghanistan nel luglio 2018, ha più volte spiegato all'opinione pubblica francese che è ora di prendere coscienza della nuova fase in cui stanno entrando gli Stati a seguito della rivoluzione tecnologica: «Siamo entrati in una nuova era. Il mondo è in uno stato di ciberguerra fredda permanente. Internet è diventato uno spazio di conflitto e di crisi. Ora, noi siamo convinti che questi scontri cibernetici potrebbero sfociare in un vero conflitto di ampiezza internazionale tra grandi potenze. La Francia ha un ruolo da spendere per evitare un'escalation»¹⁰.

5. Tutto questo lavoro non preserva certamente Parigi dagli attacchi degli altri Stati, che spesso hanno la capacità di attingere a risorse molto rilevanti, tali da rendere particolarmente complesso difendere i dati sensibili. È il caso della Cina, che da tempo cerca di sottrarre informazioni ai francesi, soprattutto per quanto riguarda il know-how industriale. Il *Figaro*, in una serie di articoli pubblicati nell'ottobre 2018, ha rivelato che la Direction générale de la sécurité intérieure (Dgsi) e la Direction générale de la sécurité extérieure (Dgse), i servizi segreti interni ed esterni, hanno scoperto dopo un lavoro di inchiesta interna durato alcuni mesi che almeno 4 mila quadri e impiegati della funzione pubblica, collaboratori di imprese strategiche e persino importanti personalità inserite nei club informali di strategia e influenza sono stati avvicinati sui social media da agenti cinesi e hanno rivelato informazioni molto sensibili, in alcuni casi compromettenti. Pechino avrebbe usato in particolare LinkedIn dove i profili falsi gestiti dalla Cina sarebbero circa cinquecento. L'obiettivo, secondo il quotidiano francese, è rubare informazioni utili per avere un vantaggio nei confronti di una potenza economica rivale «assemblando con metodo i vari pezzi di un puzzle su scala planetaria. (...) Particolarmente efficace e figlia di una metodologia rigorosa, l'azione è pilotata dal gigantesco ministero per la Sicurezza dello Stato, principale servizio civile della Repubblica Popo-

10. B. ESCHAPASSE, «David Martinon: "Le monde est en état de cyberguerre froide permanente"», *Le Point*, 2/4/2018.

lare che ospita al suo interno circa 200 mila agenti, contro circa 6 mila per la Dgse e 4 mila per la Dgsi»¹¹.

L'iniziativa cinese non ha rappresentato peraltro una sorpresa per chi si occupa di queste tematiche, visto che, come sottolineato da Sébastien-Yves Laurent, vicepresidente dell'Università di Bordeaux e voce particolarmente apprezzata del mondo tech francese, «bisogna prendere coscienza che l'economia mondiale neo-liberale fondata sulla libera circolazione espone molto più di prima a dei pericoli come lo spionaggio, l'ingerenza o la distruzione di vantaggi economici. In un mondo messo in rete, le protezioni non sono che temporanee; il solo margine realista di difesa riposa sulla sensibilizzazione degli attori economici»¹².

Ciò conferma che, se a livello di confronto tradizionale verso gli altri Stati, e cioè rispetto alla capacità di difendersi da attacchi cibernetici che sono ormai considerati praticamente convenzionali dagli ambienti militari, il paese è al passo con i tempi, non vale lo stesso per quanto riguarda la privacy e i dati messi a disposizione sui social media e in generale su Internet da parte dei cittadini francesi. La Francia, come del resto tutti gli altri Stati europei, è irrimediabilmente indietro rispetto all'alleato americano o a Stati autoritari come la Cina e la Russia, che in materia di privacy in Rete non devono rispettare le regole delle democrazie occidentali e hanno risorse sia umane che economiche difficilmente eguagliabili. Tralasciando i rapporti con Russia e Cina, i francesi cominciano a mostrare segni di insoddisfazione verso i giganti tech americani, veri e propri ricettacoli di dati e informazioni consegnati spontaneamente dagli utenti che si muovono nell'ambiente digitale. Alcuni autorevoli commentatori denunciano chiaramente la funzione di «braccio armato» della potenza americana rivestita da aziende come Facebook e Google, a dimostrazione di come la pervasività di Washington non sia benvenuta¹³.

In effetti, l'extraterritorialità del diritto americano di cui si avvalgono le aziende della Silicon Valley nei contenziosi che vertono sulla privacy e in generale sulla protezione dei dati inseriti dagli utenti su Internet pone non pochi problemi alle magistrature europee, meno capaci di intervenire in maniera efficace su queste materie. La situazione ricorda quella legata alle sanzioni contro l'Iran, contesto nel quale, pur volendo continuare a lavorare con le aziende persiane, le imprese europee sono state costrette a piegarsi alla decisione americana di ritirarsi dall'accordo sul nucleare e imporre nuove sanzioni a Teheran per evitare di incorrere in sanzioni milionarie da parte dei tribunali d'Oltreoceano.

Questo accade perché ogni transazione che avviene in valuta americana è sottoposta alla giurisdizione degli Stati Uniti, e il diritto americano diventa in alcuni casi diritto globale, con conseguente diminuzione dei margini degli altri Stati sovrani. Il Cloud Act¹⁴, varato lo scorso marzo dagli Stati Uniti, mira proprio a fare chia-

11. C. CORNEVIN, J. CHICHIZOLA, «État, entreprises: comment la Chine espionne la France», *Le Figaro*, 22/10/2018.

12. C. CORNEVIN, J. CHICHIZOLA, «Espionnage chinois: la libre circulation expose plus qu'avant à l'espionnage», *Le Figaro*, 22/10/2018.

13. M.A. COUTHERUT, «Les GAFA, bras armés de Washington?», *Les Echos*, 10/9/2018.

14. Per Cloud Act si intende il Clarifying lawful overseas use of data Act del 23/3/2018.

rezza su questo, offrendo un quadro legale sicuro per il trasferimento di prove documentali detenute nei server di società americane alle magistrature dei paesi stranieri che intendono avvalersene. L'impressione è che su questi temi Parigi non abbia la forza per contrastare lo strapotere di Washington – per inciso, i francesi non hanno fatto granché per evitare di ritrovarsi in questa situazione.

6. Più in generale, l'opinione pubblica francese comincia a capire che in questi contesti l'azione dello Stato non può essere l'unico fronte di battaglia, ma la capacità di difendere la propria sovranità passa anche da un'evoluzione culturale che deve intraprendere l'individuo. Il sottosegretario alle Politiche digitali, Mounir Mahjoubi, ha espresso chiaramente la sua frustrazione in una lunga intervista concessa a France Inter lo scorso 8 ottobre, prima nel dialogo con l'intervistatrice, e poi negli scambi con gli ascoltatori: «Gli utenti devono essere coscienti di essere responsabili dei dati che decidono di condividere su Internet. (...) Quando avete qualcosa di molto importante a casa vostra non lo lasciate davanti alla porta d'ingresso, ma lo mettete in un luogo sicuro, magari chiuso a chiave. Perché non fate lo stesso per i dati conservati in Rete? (...) Il cittadino deve rendersi conto che l'email è il mezzo di comunicazione meno sicuro al mondo»¹⁵.

Sulla stessa lunghezza d'onda si pongono i servizi segreti. Una nota congiunta della Dgse e della Dgsi sulla vulnerabilità dei cittadini francesi è esemplificativa e rende l'idea del ritardo culturale del paese. I servizi parlano di un «lungo periodo di ingenuità colpevole» e lamentano la scarsa predisposizione a adattarsi alle nuove minacce da parte degli impiegati della pubblica amministrazione: «Troppa a lungo la cultura dell'intelligence non è stata presa sul serio dai nostri concittadini come avrebbe dovuto essere. Contrariamente a quanto possiamo osservare nei paesi anglosassoni, essa è addirittura totalmente insufficiente al livello dei nostri quadri superiori e delle nostre élite politiche. Dal giugno 2017 abbiamo perciò cambiato paradigma: risponderemo alle aggressioni, colpo su colpo, quali che siano le conseguenze»¹⁶.

Il sistema giuridico francese ha tra l'altro mostrato di apprezzare le nuove norme in materia di tutela della privacy approvate nell'ultimo periodo a livello europeo e recepite dal diritto nazionale. In particolare, il nuovo regolamento europeo per la protezione dei dati, entrato in vigore il 28 maggio 2018, ha portato a un'esplosione delle denunce per violazione della privacy in Francia. Come riportato dalla Commission nationale de l'informatique et des libertés, nei primi quattro mesi di applicazione del nuovo regolamento le denunce sono aumentate del 64%, fatto che mostra una «straordinaria presa di coscienza da parte degli utenti di Internet» dei loro diritti e dei mezzi che possono tutelarli¹⁷.

15. N. DEMORAND, L. SALAMÉ, «Mounir Mahjoubi: "Nous sommes nous-mêmes responsables de nos données personnelles sur Internet"», France Inter, 9/10/2018.

16. La nota non è pubblica, ma è citata da C. CORNEVIN, J. CHICHIZOLA, «Espionnage chinois: la note d'alerte des services secrets français», *Le Figaro*, 22/10/2018.

17. A. CHERIF, «RGPD: 4 mois après, la Cnil salue la "prise de conscience inédite" des internautes», *La Tribune*, 27/9/2018.

7. È infine chiaro che una strategia francese non può prescindere da una strategia europea. Sarebbe infatti impossibile pensare che delle aziende nazionali europee in campo digitale possano competere con i quattro giganti americani Google, Amazon, Facebook e Apple, ma esistono di certo altri settori dove gli europei possono sensibilmente migliorare le proprie posizioni. Si pensi al mercato dei Bug Bounty, software per il riconoscimento e la segnalazione di bug e falle informatiche, oggi monopolizzato dalle aziende americane¹⁸. Un monopolio tra l'altro riconosciuto dalla stessa Commissione europea, che ha assegnato il bando per il suo primo programma di Bug Bounty, relativo al controllo della piattaforma di riproduzione video Vlc, largamente utilizzata dai suoi dipendenti, a Hackerone, un'azienda americana, bocciando le proposte delle concorrenti europee, giudicate non all'altezza. Una circostanza che ha fatto porre più di una domanda ai circoli informatici francesi: non è forse il caso di inserire la preferenza comunitaria per questo genere di programmi potenzialmente sensibili?¹⁹.


18. E. CAPRIOLI, *op. cit.*

19. Si vedano le osservazioni di Guillaume Tissier sul sito dell'Observatoire Fic, contenitore di riflessioni creato dalla Gendarmeria nazionale e disponibile al link bit.ly/2R6RoXe

IN INDIA INTERNET E MODERNITÀ NON SONO SINONIMI

di Prabhu GUPTARA

Il paese eccelle nelle tecnologie della comunicazione, ma la diffusione della Rete non elimina i mali antichi: diseguaglianze, corruzione e tendenze autoritarie del potere. Colpa di tenaci retaggi culturali. E di un governo che li sfrutta a suo favore.

1.  LI UTENTI DI INTERNET IN INDIA HANNO superato i 500 milioni ¹ e dal 2016 sono più di quelli statunitensi. Pertanto, l'India ha già oggi il maggior numero di «internettiani» del mondo – escludendo gli utenti dell'Internet in lingua cinese, inaccessibile a chi non sappia il mandarino.

Il numero di utenti donne in India è tuttavia limitato: appena 143 milioni. Questa sproporzione non è un fenomeno solo indiano e ha varie ragioni, sovente collegate a fattori religiosi e culturali. Paradossalmente, malgrado il politeismo che caratterizza il grosso dell'India, il paese vede una diffusa discriminazione di genere, di matrice religiosa e culturale. Tanto che alcuni studi considerano l'India il paese più pericoloso al mondo per le donne ².

Malgrado ciò, il mercato dell'Internet indiano dovrebbe continuare a crescere, data l'enorme popolazione del paese: 1,3 miliardi di persone. Nel dicembre 2017 gli utenti erano il 64,84% della popolazione urbana adulta (rispetto al 60,6% dell'anno prima), ma solo il 20,26% della popolazione rurale adulta (18% nel 2016). Ciò lascia un margine di circa 160 milioni di potenziali nuovi utenti nelle zone urbane e di ben 732 milioni nelle campagne.

Non è solo il numero degli internettiani indiani a crescere, ma anche il loro uso della Rete: si stima che oggi siano 281 milioni quelli che vi accedono giornalmente, per un tempo medio che aumenta costantemente e oggi si situa sui 73 minuti ³. Nell'India urbana, l'86% degli utenti usa Internet per comunicare, l'85% per l'intrattenimento, il 70% per coltivare rapporti sociali, il 44% per transazioni commerciali

1. S. AGARWAL, «Internet Users in India Expected to Reach 500 Million by June: IAMAI», *The Economic Times*, 20/2/2018.

2. «Factbox: Which Are the World's 10 Most Dangerous Countries for Women?», *Reuters*, 26/6/2018.

3. «Average Time Spent per Day with Major Media by Adults in India, 2017 (hrs:mins)», *eMarketer*, 14/11/2017.

e finanziarie e il 35% per i servizi online. Per contro, nelle aree rurali l'intrattenimento è la prima forma d'uso (58%), seguita dai social network (49%), i servizi online (35%) e le transazioni economico-finanziarie (16%). Per accedere a Internet, la maggior parte degli indiani usa gli smartphone (in India ve ne sono 530 milioni).

Anche i social media sono sempre più diffusi⁴: Facebook e YouTube, che guidano la classifica indiana per quantità di contenuti generati dagli utenti⁵, hanno ciascuno circa 220 milioni di utenti stimati nel paese⁶. Ne deriva tra l'altro che l'India è una delle piazze di e-commerce a più rapida crescita, con circa due miliardi di transazioni giornaliere⁷.

Più importante degli utenti è il numero degli ingegneri informatici. È arduo fornire cifre attendibili, perché nel mondo non vi è una definizione accademica univoca di «ingegnere informatico» o «sviluppatore di software». Tuttavia, è indubbio che gli Stati Uniti ne abbiano il maggior numero (probabilmente sui 4,4 milioni⁸), seguiti dalla Cina. L'India è però il paese in cui questa figura risulta in più rapida crescita e si appresta a superare America e Cina al più tardi entro il 2023⁹. Già oggi, il 75% dei talenti digitali del mondo vive in India¹⁰.

Questa vitalità è del resto attestata dal fatto che un terzo degli sviluppatori di software della Silicon Valley californiana è di origine indiana, mentre un'analoga percentuale di start-up tecnologiche della stessa Silicon Valley e l'8% delle aziende high-tech di tutti gli Stati Uniti risultano fondate da persone di origine indiana, pur rappresentando queste solo l'1% della popolazione statunitense.

L'India è una delle principali mete della tecnologia e dei servizi connessi: nel 2017-18 essa ha attratto il 55% delle delocalizzazioni di servizi tecnologici a livello globale, un mercato da 190 miliardi di dollari l'anno¹¹. Le stesse aziende tecnologiche indiane hanno aperto oltre mille filiali in circa 80 paesi.

La crescita del ruolo indiano in Internet si è tuttavia accompagnata a un aumento della criminalità informatica, al punto che questa produce oggi danni per oltre 4 miliardi di dollari l'anno¹². L'India è il secondo paese al mondo per vulnerabilità al crimine informatico¹³ e le sue aziende sono al sesto posto nella triste classifica delle più colpite da questo genere di attacchi¹⁴. Tra le vittime figurano banche, aziende di servizi pubblici, compagnie di telecomunicazioni e gestori di altre infrastrutture critiche, comparti della Difesa e altri settori governativi.

4. «Number of Social Network Users in India From 2015 to 2022 (in Millions)», *Statista*, 2018.

5. «Penetration of Leading Social Networks in India as of 3rd Quarter 2017», *Statista*, 2018.

6. «Number of Facebook Users in India from 2015 to 2022 (in Millions)», *Statista*, 2018.

7. «Retail E-Commerce Sales CAGR Forecast in Selected Countries from 2018 to 2022», *Statista*, 2018.

8. *Global Developer Population and Demographic Study 2018*, vol. 2, Evans Data Corporation, 2018.

9. *Ibidem*.

10. «IT & ITes Industry in India», India Brand Equity Foundation, agg. a ottobre 2018.

11. *Ibidem*.

12. «ACI Worldwide and AGSTTL Highlight Megatrends Shaping India's Digital Payments Revolution – By 2025, Digital Transactions Could Be Worth \$1 Trillion Annually», ACI Universal Payments, 12/3/2018.

13. *Internet Security Threat Report 2018*, Symantec, goo.gl/NqQhv7

14. N. RAJAN, «Symantec Report: Cybercriminals Love Indian Enterprises, Social Media Adding Fuel to Fire», *The Indian Express*, 24/4/2016.

Finalmente, sebbene con ritardo, si è preso atto del problema¹⁵ e il governo sembra intenzionato a prendere provvedimenti per proteggere i settori civile e militare¹⁶.

Negli ultimi cinque anni, la crescita della criminalità informatica ha inoltre obbligato le aziende indiane a investire sempre più nei sistemi di protezione, facendo crescere il settore del 25% all'anno¹⁷. Le tecnologie per la difesa informatica, tuttavia, risultano meno avanzate e sofisticate rispetto a quelle utilizzate dagli hackers, e per la maggior parte delle aziende indiane la *cybersecurity* resta una questione meramente tecnologica, più che una strategia di business su cui concentrarsi.

2. Quanto sopra espone un curioso paradosso: l'India miete successi nei campi connessi a Internet, ma questi ambiti alimentano lo scontento degli stessi indiani, che lamentano nepotismo¹⁸, scarsa qualità dell'occupazione ed etica aziendale inadeguata.

Il fatto è che a parte le eccezioni – menti brillanti del calibro di Sundar Pichai (Google) e Satya Nadella (Microsoft) – molti indiani seguono ancora norme sociali tradizionali, che generano comportamenti poco virtuosi. In Occidente si può essere considerati bugiardi, o quantomeno inaffidabili, non solo se si dice il falso, ma anche se si omette di dire esattamente come stanno le cose. C'è poi l'eredità del sistema castale, per cui molti indiani preferiscono lavorare con persone dello stesso gruppo sociale e linguistico. Infine, l'arrivismo che caratterizza il settore informatico aumenta esponenzialmente le aspettative familiari e spinge i singoli a fare di tutto per riuscire.

Eppure, le attitudini indiane stanno cambiando, uniformandosi alle norme internazionali. La versione indiana del movimento #MeToo, ad esempio, non è spuntata dal nulla: è piuttosto il risultato di una lunga gestazione iniziata negli anni Novanta e appare persino più ampio ed esplosivo dei corrispettivi occidentali¹⁹.

I modelli sociali in rapido mutamento riflettono del resto i cambiamenti demografici: la popolazione indiana è sempre più dominata dai giovani, che sono sempre più refrattari ad abbracciare i valori tradizionali.

Ma il problema più grave è quello della corruzione, una sfida ardua da vincere in India e un tipico caso di inversione storica dopo l'interludio vittoriano del periodo coloniale²⁰. Anche la qualità del lavoro è un problema serio, in parte a causa della concezione indiana ciclica del tempo: le lingue usate dal grosso degli indiani usano la stessa parola per «ieri» e «domani». Altrettanto rilevante è l'inadeguata istruzione di quelli che, in teoria, dovrebbero essere qualificati. Il problema ha

15. V.K. SARASWAT, *Cyber Security*, goo.gl/nmhFv

16. S. DHARMARAJ, «The Current State of Cyber Security in India», *Open Gov*, 1/8/2018.

17. C. CASTELLI, B. GABRIEL, J. YATES, P. BOOTH, *Strengthening Digital Society Against Cyber Shocks – Key Findings from The Global State of Information Security Survey 2018*, Price Waterhouse Coopers, 2017.

18. A. BHATTACHARYA, «The US Says Oracle Is Encouraging Indians to Hire Other Indians – and It's Killing Diversity», *Quartz India*, 19/1/2017.

19. «#MeToo's Twitter Gatekeepers Power a People's Campaign in India», *Bloomberg*, 23/10/2018.

20. P. GUPTARA, «Can We Stop Misgovernance in India?», *Fair Observer*, 26/9/2018.

assunto visibilità internazionale nel 2005, quando un rapporto McKinsey asserì che solo il 25% degli ingegneri indiani era effettivamente impiegabile. Attualmente, si dibatte se i laureati impiegabili siano il 53% o appena il 6%²¹.

La differenza abissale tra le due stime evidenzia un altro problema dell'India: l'attendibilità dei numeri e, in generale, dell'informazione²². Non vi è certezza sui tassi di crescita (oltre l'8%) esibiti dal governo, presi acriticamente per buoni da reputate istituzioni internazionali come la Banca mondiale, a dispetto della realtà vissuta dagli indiani. Nell'Environmental Performance Index, stilato congiuntamente dalle università di Yale e Columbia in collaborazione con il World Economic Forum, l'India è 117ª su 180 paesi. Nell'Indice di sviluppo umano dell'Onu (che guarda all'istruzione e alla salute, oltre che al pil pro capite), l'India è 130ª, mentre l'indice sulla facilità del fare impresa colloca il paese al 100° posto. Viceversa, l'India fa molto bene nella classifica mondiale degli omicidi (seconda), della schiavitù (quarta), dei senza casa (ottava) e della spesa militare (quinta su 186). Questi indici descrivono peraltro la posizione di un paese rispetto agli altri, sicché spesso celano realtà numeriche rilevanti, come il fatto che l'India abbia più poveri assoluti (che vivono cioè con meno di mille dollari l'anno) di tutti gli altri Stati eccetto la Nigeria; o che il rapporto medio tra dottori e popolazione nel paese sia di uno a 11.082: dieci volte meno di quanto raccomandato dall'Organizzazione mondiale per la sanità. La spesa sanitaria pro capite dell'India ammonta ad appena 3 rupie (meno di cinque centesimi).

Da tutto ciò si evince che l'«India scintillante» (*shining India* è lo slogan promozionale del paese) è appannaggio di quell'1% che detiene il 73% della ricchezza nazionale. Parliamo di 13,5 milioni di persone: tante in termini assoluti, pochissime in confronto al resto. La vera classe media – comparabile a quella occidentale – è costituita dal successivo 9% della popolazione, il che lascia fuori dal «miracolo» il restante 90%.

Uno straniero che arriva per la prima volta in una metropoli indiana può essere facilmente colpito dalla relativa abbondanza di autostrade ben tenute, auto di lusso, alberghi di alta categoria, centri commerciali di stampo occidentale e sedi all'avanguardia di grandi multinazionali indiane attive nel campo delle nuove tecnologie. Tuttavia, per la «vera India» – oltre un miliardo di persone – la vita è segnata da povertà, malnutrizione, malattie, analfabetismo, disoccupazione e mancanza di opportunità. Per queste moltitudini, crescita è sinonimo di espropriazione del poco che hanno, in particolare terra, aria buona e acqua pulita, divorate dall'avanzata di finanza e mercato²³. Lo stato penoso di gran parte delle infrastrutture è

21. P. GUPTARA ET ALII (a cura di), *Where Did We Go Wrong? Reflections on 200 years of Modern Education in India*, di prossima uscita.

22. A. DATAR, «The Four Problems with Economic Data in India», *Bloomberg*, 2/9/2018; D. DATTA, «How Trustworthy Is India's Economic Data? Does the Modi Government Care About It Anymore?», *Scroll.in*, 31/9/2018.

23. A. ASHRAF, «Why Congress Should Tie up with JAYS, the Adivasi Movement in MP That Began on Facebook», *The Wire*, 20/10/2018; I. MARLOW, «World's Fastest Growing Economy Has the World's Most Toxic Air», *The Economic Times*, 22/10/2018; N. LAL, «Water Scarcity: India's Silent Crisis», IPS (Inter Press Service), 16/3/2018.

del resto evidente – siano strade, porti, aeroporti o reti di telecomunicazioni. L'attuale strategia governativa, consistente nell'applicare soluzioni high-tech a infrastrutture decadenti, non risolve il problema. Anzi, lo complica²⁴.

3. Negli anni, il governo indiano ha intrattenuto un rapporto ambivalente con le aziende digitali. Gli investitori esteri sono accolti con pacche sulle spalle e invitati alle fiere. Ma si sospetta di ogni straniero. La condotta che ne consegue risulta spesso confusa e sgradevole²⁵. Il risultato è che molti investitori sbarcati in India con forti aspettative se ne sono andati, oppure sono in balia di alterne fortune. Tra gli esempi si possono citare la francese Carrefour, la tedesca Fraport, la statunitense General Motors, la norvegese Telenor e la Royal Bank of Scotland.

Parte del problema origina dall'approccio tradizionalmente ambiguo dell'India all'informazione. Questa è un bene prezioso, dunque è stata monopolizzata dalla casta dominante (i bramini), che rappresentano circa il 5% della popolazione. L'informazione è stata nascosta il più possibile agli stranieri e alle caste inferiori, cui appartiene circa il 95% degli indiani. Si tratta di una costante negativa che risale alle antiche autorità religiose.

Sebbene l'informazione sia indispensabile agli affari e al governo, l'attuale esecutivo sta erodendo la libertà di stampa²⁶ e le informazioni ottenibili in virtù del Right to Information Act. Ciò si deve in parte al fatto che il governo in carica rive-risce le autorità religiose al punto da invocarle regolarmente con mantra del tipo «Internet esisteva al tempo del Mahabharata»²⁷ (3000 a.C circa), o «la scienza e il volo interplanetario furono padroneggiati dagli indiani tra il 1500 e il 500 a.C.» (co-sì il primo ministro²⁸).

Le vecchie attitudini si rinvergono anche nei roboanti annunci di nuovi progetti, come Digital India, Smart Cities e National Optical Fibre Network, cui segue l'incapacità di garantire cose semplici e vicine al quotidiano della gente, come un Gange pulito. La realizzazione dei progetti è da sempre un problema in India, anche sotto il profilo giuridico. Ne è esempio emblematico la lotta ingaggiata dalla società civile contro Aadhaar, il più grande progetto biometrico al mondo che assegna a ogni indiano un numero di 12 cifre prodotto in base a dati raccolti dalla Unique Identification Authority of India (Udai). Nel settembre 2018, la Corte suprema ha statuito che la carta Aadhaar non è obbligatoria, ma nonostante ciò il governo continua a spingere i cittadini a collegare il loro numero Aadhaar con le

24. M. CHARI, «India's E-Migrate Website Continues to Hurt Workers Seeking Gulf Jobs, Say Agents and Labourers», *Scroll.in*, 22/10/2018.

25. V. GOEL, «India Pushes Back Against Tech "Colonization" by Internet Giants», *The New York Times*, 31/8/2018; S. AGARWAL, «India Will Put Facebook in the Dock if Needed: Ravi Shankar Prasad», *The Economic Times*, 22/3/2018.

26. P. GUPTARA, «Press Freedom in India under Prime Minister Narendra Modi», *Research Gate*, novembre 2014.

27. B. SINGH, «Internet Existed in the Days of Mahabharata: Tripura CM Biplab Deb», *The Economic Times*, 18/4/2018.

28. M. RAHMAN, «Indian Prime Minister Claims Genetic Science Existed in Ancient Times», *The Guardian*, 28/10/2014.

schede sim dei cellulari, i conti correnti, il fondo di previdenza sociale e molti altri servizi. Le associazioni per i diritti civili osteggiano Aadhaar per ragioni di privacy²⁹, in parte accolte dalla Corte suprema con la sentenza del 24 agosto 2017³⁰ che ha definito la riservatezza un diritto fondamentale. Tale sentenza tende ad allineare il sistema legale indiano a quello europeo, che ha visto la recente approvazione del nuovo regolamento sulla privacy (General Data Protection Regulation).

4. Uno sforzo molto più concertato volto alla regolamentazione di Internet in India è stato pubblicamente giustificato con la necessità di contrastare la diffusione della disinformazione, delle bufale, delle pratiche denigratorie e più in generale l'intero modello di business basato sulla raccolta dei dati personali per indirizzare la pubblicità e farci passare sempre più tempo su Internet, comprando e consumando sempre più. In realtà, molte delle nuove norme usano la diffusione di Internet per accentuare pratiche centralistiche e autoritarie, al fine di ridurre la trasparenza e la responsabilità del governo verso i cittadini. Ciò appare in linea con il parziale ritiro dell'India dalla globalizzazione coinciso con l'avvento di Modi, nel 2014, e con l'aumento di protezionismo e accentramento³¹.

I nuovi requisiti per la localizzazione dei dati, ad esempio, limitano la ricerca e caricano piccole imprese e start-up di ulteriori oneri burocratici³²; al contempo, accrescono le capacità di sorveglianza dello Stato³³, che ora può accedere liberamente a tutte le informazioni personali degli indiani, sia in patria che all'estero.

L'India ha fatto degli sforzi per scrollarsi di dosso gli aspetti più indesiderabili della sua cultura, anche da prima dell'indipendenza dall'Inghilterra nel 1947. Ma i retaggi persistono, forti. Il 70% della popolazione è ancora profondamente svantaggiato dalla storica discriminazione a danno degli intoccabili e delle caste inferiori. La tigre della modernità non ha ancora avuto la meglio sul risorgente elefante della tradizione.

(traduzione di Fabrizio Maronta)

29. «UID an Assault on Individual Liberty: Activists», *Rediff Business*, 6/9/2010.

30. goo.gl/Fs19qH

31. N. KWATRA, «Is India a Tariff King?», *Live Mint*, 16/10/2018; P. GUPTARA, «How Tensions Between Delhi and India's Numerous States Might Cripple the Union», *MacroGeo*, 23/2/2017.

32. N. CHRISTOPHER, «India's Data Protection Bill Is Poorly Worded; Does not Serve Any Stakeholder's Interests», *The Economic Times*, 4/10/2018.

33. D. GILBERT, «India's New Data Protection Law Could Create a Massive Surveillance State», *Vice News*, 7/9/2018.



LA RETE A STELLE E STRISCE

Parte III


CIBERGUERRA **TERRA *di* NESSUNO?**

L'AMERICA ALL'OFFENSIVA CIBERNETICA

di Federico PETRONI

Le ciberguerre non rivoluzionano i rapporti di forza, ma accorciano le distanze fra Usa e rivali. Non disponendo di uno scudo sicuro, Washington si racconta all'attacco per ricordare a sé e al mondo la superiorità anche nella quinta dimensione.

*Stiamo vagando
in un territorio oscuro.*
Robert Gates

1.  NELLO SPAZIO CIBERNETICO GLI STATI UNITI hanno un vantaggio sui rivali meno assoluto rispetto a quello di cui godono nelle dimensioni classiche della potenza. Ma la competizione nel ciberspazio, benché più accesa che altrove, non è comunque sufficiente da sola a minare il primato americano. In questa doppia considerazione sta la cifra della postura di Washington nel cosiddetto quinto dominio, l'ultimo abbracciato dai circoli strategici dopo terra, mare, aria e cosmo. Forse il più nebuloso, ma non certo il meno sfruttato né quello con minori ricadute sulle quotidiane schermaglie fra potenze.

L'idea che nella guerra cibernetica la forbice con gli avversari sia ridotta può sembrare curiosa, di fronte alla portata planetaria delle aziende tecnologiche a stelle e strisce, al relativo potenziale di intercettazione e attacco e alla disponibilità di gran parte delle infrastrutture della connessione (cavi, centri di stoccaggio dei dati eccetera). Eppure, per descrivere la proiezione strategico-militare degli Stati Uniti in questa sfera non si sfoggiano termini come presidio, controllo, supremazia, invece impiegati in ambito marittimo, per esempio per i principali colli di bottiglia.

Nel ciberspazio le distanze sono inferiori per l'inerte conformazione di questo territorio oscuro, dove offesa e confusione hanno la meglio su difesa e certezza. Perché i rivali approfittano delle ignote vastità di Internet per sfidare la superpotenza in modi altrimenti inimmaginabili. Per imporle costi e danni sconosciuti in altre dimensioni della competizione strategica. Fino a instillarle il dubbio sull'affidabilità dei propri armamenti e delle proprie istituzioni. Tanto che a Washington non si può più prescindere dall'abuso della parola d'ordine «Pearl Harbor cibernetica» per ottenere da un Congresso analfabeta digitale fondi per qualunque programma di sicurezza informatica. È ormai moneta corrente la consapevolezza che gli avversari dell'America hanno iniziato a colmare il divario nella ciberguerra a un

passo più rapido di quanto non ci si aspettasse all'alba dell'età di Internet. E, versando amaro pianto di cocodrillo, ci si chiede se a inizio anni Dieci, con il sabotaggio delle centrifughe nucleari iraniane, gli Stati Uniti non abbiano inconsapevolmente dato il la a una corsa agli armamenti e a un loro disinibito impiego oltre le proprie capacità di contenerli.

Non bisogna tuttavia farsi contagiare dagli isterismi delle Cassandre d'Oltreoceano, in particolare vista la coincidenza fra chi annuncia l'apocalisse e chi ci lucra sopra. Così come l'analisi geopolitica rifugge il determinismo geografico, la valutazione sul grado di potenza degli Stati Uniti nel ciberspazio deve partire dalla considerazione che la Rete non ha per il momento rivoluzionato i rapporti di forza. Solo così si potranno cogliere e relativizzare i fattori che, semmai, li avvicinano. E considerare come il Numero Uno si stia attrezzando per rimanere tale anche in questa dimensione.

2. Avrò anche cambiato il mondo, ma Internet non ha (ancora) stravolto la competizione fra potenze. Non ha introdotto requisiti di superiorità tali da prevalere su altri fattori. Piuttosto, aggiunge vettori di influenza e attacco; si affianca, completandoli e accelerandoli, ai metodi tradizionali con cui sulla scena mondiale gli avversari si contendono potere e risorse. «Le operazioni cibernetiche», scrivono Brandon Valeriano, Benjamin Jensen e Ryan C. Maness, docenti i primi due alla Marine Corps University e il terzo alla Naval Postgraduate School, «non alterano il gioco fra le grandi potenze o le gerarchie inerenti ai sistemi di rivalità regionali. Nell'età digitale continuano a trionfare realtà politiche consolidate, rendendo difficile da una prospettiva strategica (attuare) un cambiamento rivoluzionario». Aggiungendo che «solo costosi e complessi attacchi cibernetici di degradazione progettati per minare le reti avversarie tendono a produrre effettivi coercitivi. Ci sono poche vittorie decisive nella dimensione digitale». Anche perché gli Stati vi ricorrono soprattutto «per mandare segnali e compiere furti allo scopo di plasmare una competizione di lungo periodo»¹.

Sin qui nella Rete abbiamo assistito non a una sostituzione, ma a un trasferimento di gerarchie e rivalità già presenti. Così, per esempio, quasi nessuna linea di faglia attuale è esente da massicce operazioni cibernetiche o, meglio, da quelle che superano il mero ambito della criminalità per abbracciare una dimensione strategico-militare, dallo spionaggio alla distruzione di dati o infrastrutture. Allo stesso modo, la possibilità di impiegare Internet a scopo strategico non ha creato nuovi villani statuali, non ha aggiunto nuove nazioni alla rosa dei nemici dell'America. Il cui bestiario cibernetico è del tutto speculare a quello tradizionale, ugualmente composto da Cina, Russia, Iran e Corea del Nord. Una ciberpotenza non s'impromette. E nemmeno una canaglia.

Concentrandosi sugli Stati Uniti, questi ultimi traducono nell'ambito digitale alcuni dei pilastri del proprio primato globale, stampo per forgiare vantaggi infor-

matici. Così inquadrata, è la vasta rete di alleati, soci e clienti a rendere possibile l'irradiazione di software e hardware a stelle e strisce e degli usi spionistici a essi connessi. È l'impareggiato – benché rissoso: vedi i litigi fra Silicon Valley e Washington – complesso militare-industriale ad aver creato Internet, dato impulso allo sviluppo di colossi come Google e a fornire ad agenzie d'intelligence e Forze armate le armi cibernetiche, manufatte come ogni altro strumento bellico dalla pleora di *contractors*. Ancora, è l'estroversione della società e della nazione ad assimilare i cervelli necessari a mantenere innovativa la scienza applicata *made in Usa*. Ed è la ancora superiore capacità di raccontarsi e di rendere attraente il proprio stile di vita a spingere mezzo mondo a dotarsi di dispositivi americani per connettersi e a cedere i propri dati a social network ugualmente americani.

A rimarcare la subordinazione del primato tecnologico al momento geopolitico è la concomitanza, solo apparentemente casuale, fra l'invenzione del World Wide Web al Cern di Ginevra e la caduta dell'Urss, entrambe datate 1991. L'universalizzazione dei protocolli con cui si naviga in uno spazio aperto dagli statunitensi sarebbe stata possibile solo in un mondo in cui gli stessi americani si erano ormai convinti di aver fermato le lancette della storia. Nella lucidissima consapevolezza del servizio d'intelligence chiamato a occuparsi di questa sfera, la National Security Agency (Nsa), che tale diffusione avrebbe reso praticamente ubiqua le proprie attività di intrusione. Internet non ha universalizzato l'impero americano. Semmai, è il contrario.

Gli Stati Uniti trasferiscono alla dimensione cibernetica anche peculiari aspetti della propria mentalità strategica. Le ciberguerre toccano una corda molto sensibile della psicologia americana, poiché offrono l'illusione di sconfiggere l'avversario senza pagare un caro prezzo di sangue e denaro, senza scomodarsi da casa, senza incuriosirsi del mondo, sporcandosene di conseguenza le mani. Il fascino per le armi di questo tipo è storico², deriva dalla guerra elettronica e si è sviluppato quando negli anni Settanta, in pieno sforzo di compensazione dei vantaggi bellici dell'Unione Sovietica, gli strateghi del Pentagono si resero conto che le battaglie dei computer promettevano di colpire il nemico a livello strategico. Non solamente disturbandone i segnali, ma impedendogli di condurre le operazioni (la cosiddetta *counter-command and control warfare*, in pentagonese). Concetti poi testati nella guerra del Golfo del 1990-91, immaginato sigillo dell'onnipotenza statunitense.

La stessa fissazione è riscontrabile per la missilistica di precisione, per i droni, per l'arma atomica sganciata su Hiroshima e Nagasaki per piegare un altrimenti indomito avversario giapponese. Vincere velocemente e in modo decisivo: il sogno di ogni inquilino della Casa Bianca. Per questo le armi cibernetiche sono state impiegate di recente come mezzi coercitivi a un passo dall'uso della forza, per sottrarsi al dilemma di non potere davvero ricorrere alla guerra conclamata. È stato il caso tanto del virus Stuxnet, lanciato per fermare la corsa al nucleare dell'Iran³,

2. Eccellente e dettagliata la ricostruzione di F. KAPLAN, *Dark Territory: The Secret History of Cyber War*, New York 2016, Simon & Schuster.

3. D.E. SANGER, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York 2012, Crown Publishers, pp. 188-225.

quanto dello sforzo per disarticolare il programma missilistico della Corea del Nord, che nel 2016 vide fallire sette degli otto test sui Musudan in circostanze ancora non del tutto chiarite⁴.

3. Il primato digitale dischiude enormi possibilità per conservarsi in vetta al mondo. Tuttavia, espone a vulnerabilità altrettanto vaste. Esattamente come l'estroversione dell'impero americano comporta un fardello per le classi meno abbienti⁵, la connessione con il resto del pianeta impone alla nazione costi sostanziosi in termini di sicurezza.

I computer si dividono fra quelli che sono stati hackerati e quelli che lo saranno, recita uno degli adagi più diffusi fra gli esperti del settore. A marcare una caratteristica genetica delle operazioni cibernetiche: il pressoché incancellabile vantaggio dell'offesa sulla difesa. Non esiste un argine affidabile nei confronti di un attaccante dotato di soldi e pazienza per scovare una porta sul retro lasciata aperta, la cosiddetta *backdoor*, nel sistema informatico messo nel mirino. L'esistenza stessa di una rete prevede la possibilità di accedervi da molteplici e ingovernati punti d'ingresso, come notava un rapporto della Rand Corporation, think tank legato all'Aeronautica, già nel 1967, due anni *prima* della nascita di Internet⁶. Nella sintesi non estranea a una certa vanità di un anonimo funzionario di un'agenzia d'intelligence americana: «Se riesci a immaginarlo, puoi farlo. Serve solo tempo, denaro e un po' di impegno»⁷.

Tale sbilanciamento è dovuto a diversi fattori. Innanzitutto, la capacità di negare il proprio coinvolgimento negli attacchi – l'analisi forense riesce a individuare i responsabili, il difficile è ricondurli a un apparato statale. Le armi cibernetiche sono poi più efficaci nell'area grigia a un passo dall'aperta ostilità e pertanto incentivano azioni di disturbo. Inoltre, gli strumenti, le operazioni e le dottrine impiegati per attaccare sono spesso estremamente simili a quelli adoperati per difendersi – quando non coincidenti. Studiare l'avversario per capire come proteggersi può imporre un'intrusione nelle sue reti. Siamo in pieno dilemma della cibersicurezza, come lo chiama lo studioso Ben Buchanan⁸: quando si individua un intruso nei propri sistemi, è impossibile stabilire con certezza e soprattutto in anticipo chi sia e quali siano le sue intenzioni. Infine, il costo d'ingresso sul palcoscenico delle ciberguerre è elevato – specie in termini di pazienza richiesta: la criminalità organizzata ha obiettivi molto più remunerativi e fulminei – ma ridotto e immediatamente spendibile rispetto ad altri attributi della potenza. L'esempio più lampante è quello della Corea del Nord, che ha fatto fare il salto di qualità al proprio

4. D.E. SANGER, W.L. BROAD, «Trump Inherits a Secret Cyberwar Against North Korean Missiles», *The New York Times*, 4/3/2017.

5. D. FABBRI, «Trump e i dolori della giovane superpotenza», *Limes*, «L'agenda di Trump», n. 11/2016, pp. 33-44.

6. Cit. in F. KAPLAN, *op. cit.*, pp. 8-9.

7. A. SEGAL, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York 2016, Public Affairs, p. 38.

8. B. BUCHANAN, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, Oxford 2017, Oxford University Press.

GERARCHIA DELLE POTENZE CIBERNETICHE

POSIZIONE	PAESE	CIBERDIFESA	CIBERATTACCO	CIBERDIPENDENZA	CAPACITÀ MEDIE DI CIBERSICUREZZA
1	Usa	9,5	8,95	1,1	6,52
2	Cina	7,06	7,67	4,4	6,38
3	India	6,06	3,06	6,5	5,21
4	Francia	7,54	4,24	3,2	4,99
5	Germania	7,43	5,32	2,1	4,95
6	Italia	6,17	3,73	4,7	4,87
7	Russia	6,84	4,63	2,95	4,81
8	Brasile	5,56	3,37	5,2	4,71
9	Corea del Nord	3,07	0,82	9,5	4,46
10	Turchia	5,18	2,27	5,85	4,43
11	Giappone	7,01	5,77	0,45	4,41
12	Israele	7,18	2,92	2,85	4,32
13	Canada	6,18	4,01	2,55	4,25
14	Regno Unito	7,56	4,56	0,5	4,21
15	Corea del Sud	6,28	4,38	1,7	4,12
16	Iran	3,21	1	7,05	3,75

Fonte: Çeliktaş e Ünlü, Itu, 2018

Ufficio 121 solamente dopo l'avvento di Kim Jong-un, mentre il programma nucleare è ben più datato.

Anche Washington è impegnata nello stesso tipo di operazioni e con capacità senza dubbio superiori. Tuttavia, è chiaro che lo squilibrio difesa-offesa va a danno di chi è nella posizione di essere sfidato. «Per almeno i prossimi cinque-dieci anni, le capacità cibernetiche offensive dei nostri avversari potenziali più abili probabilmente supereranno di gran lunga la capacità degli Stati Uniti di difendere e di rafforzare adeguatamente la resilienza delle nostre infrastrutture fondamentali», è la fosca previsione di un rapporto del 2017 del Defense Science Board del Pentagono⁹.

Nulla può davvero dirsi al sicuro negli Stati Uniti, paese che vanta un terzo degli indirizzi Ip del pianeta (1,6 miliardi): indice di potenza, essendo cinque volte maggiore rispetto alla Cina, ma pure di penetrabilità, con la società a stelle e strisce ineguagliata per numero di infrastrutture e apparecchi connessi alla Rete. Esposizione sfruttata dai rivali per compromettere diversi sistemi informatici sensibili. Nel marzo 2018, Fbi e dipartimento per la Sicurezza interna hanno denunciato una ramificata campagna di infiltrazione di hacker russi nelle infrastrutture vitali del paese, rete elettrica e centrali nucleari comprese¹⁰. Nell'ottobre 2018, l'ufficio di

9. «Task Force on Cyber Deterrence», Defense Science Board, U.S. Department of Defense, febbraio 2017, p. 4.

10. «Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors», U.S. Computer Emergency Readiness Team, *Alert* (Ta18-074A), 16/3/2018.

supervisione del governo del Congresso ha ammonito che «quasi tutti i principali programmi di acquisizione (di armamenti) testati fra 2012 e 2017 avevano vulnerabilità cibernetiche che gli avversari possono sfruttare». Riprendendo un Pentagono «non pienamente a conoscenza di tutte le vulnerabilità cibernetiche dei propri sistemi d'arma»¹¹.

La vera posta in gioco è lo sgretolamento della fiducia nelle proprie difese. «Gli Stati Uniti non possono essere sicuri che i sistemi delle nostre tecnologie informatiche essenziali funzioneranno in caso di attacco», paventava nel 2013 il Defense Science Board. A cinque anni di distanza, la valutazione è se possibile peggiorata: «Le misure tecniche di cibersicurezza (...) non possono di per sé fornire sufficiente fiducia nell'affidabilità dei sistemi vitali, inclusi quelli delle armi nucleari», riscontra un rapporto della Nuclear Threat Initiative¹².

Anche facendo la tara all'enfasi tipica di un ambito in cui è quasi impossibile essere smentiti, non si può non notare che persino le stesse armi cibernetiche, fra i segreti più reconditi della superpotenza, possono essere oggetto di furto. Come successo all'ormai ex unità d'élite dell'Nsa, la Tailored Access Operations che si è vista trafugare ed esporre al pubblico dominio alcuni dei codici impiegati nelle missioni più disparate per mano di uno o più hacker sotto il nome di Shadow Brokers. Virus poi ritortisi contro l'America stessa, impiegati nel vasto e indiscriminato attacco cibernetico WannaCry del 2017 attribuito alla Corea del Nord. Nella dolorosa ammissione di uno degli operatori: «È come lavorare per la Coca-Cola e scoprire un giorno che qualcuno ha messo la sua ricetta segreta su Internet»¹³.

A peggiorare il quadro delle difese cibernetiche è la confusione burocratica. Non esiste in America una singola autorità responsabile in questo settore. Nsa e Comando cibernetico del Pentagono forniscono consulenza, ma sono assorbiti da missioni spionistico-militari. Il compito spetterebbe al dipartimento per la Sicurezza interna, ma si tratta più che altro di coordinamento. La protezione dei 16 tipi di infrastrutture vitali pertiene a otto enti diversi, peraltro tutti fuorché uno (la Difesa) estranei al mestiere e cronicamente privi del personale sufficiente per la missione.

L'impresa, peraltro, è titanica: andati sono i tempi degli anni Novanta in cui il traffico Internet americano fluiva attraverso due soli *edifici*, uno sulla costa Est e uno su quella Ovest. Oggi, il Cyber Command fatica a presidiare la decina scarsa di punti d'accesso delle reti militari, figurarsi le migliaia in mano ai gestori di snodi vitali – negli Stati Uniti il 90% del flusso dei dati avviene attraverso infrastrutture di proprietà di aziende come Verizon e At&T. Privati che a loro volta fino a non troppo tempo fa ritenevano meno oneroso riparare i danni subiti da un ciberattacco piuttosto che spendere fortune nel prevenirne uno. Tanto da spingere il segretario

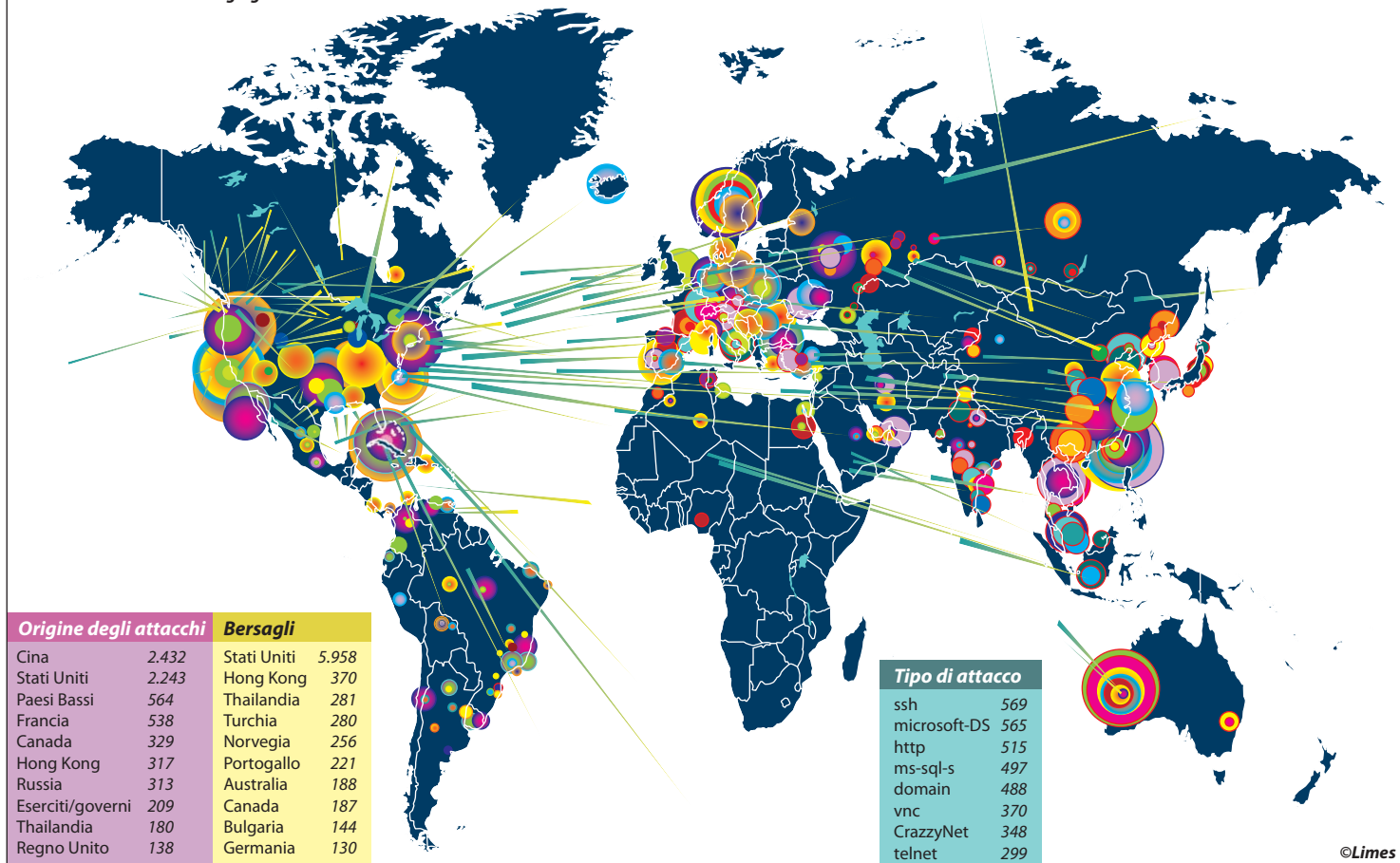
11. Entrambe le citazioni in «Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities», U.S. Government Accountability Office, Gao-19-128, ottobre 2018, rispettivamente alle pp. 21 e 25.

12. Le citazioni rispettivamente in «Resilient Military and the Advanced Cyber Threat», Defense Science Board, U.S. Department of Defense, gennaio 2013, p. 1 e P.O. STOUTLAND, S. PITTS-KIEFER, «Nuclear Weapons in the New Cyber Age», Nuclear Threat Initiative, settembre 2018, p. 10.

13. D.E. SANGER, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, London 2018, Scribe, ed. Kindle, pos. 3759.

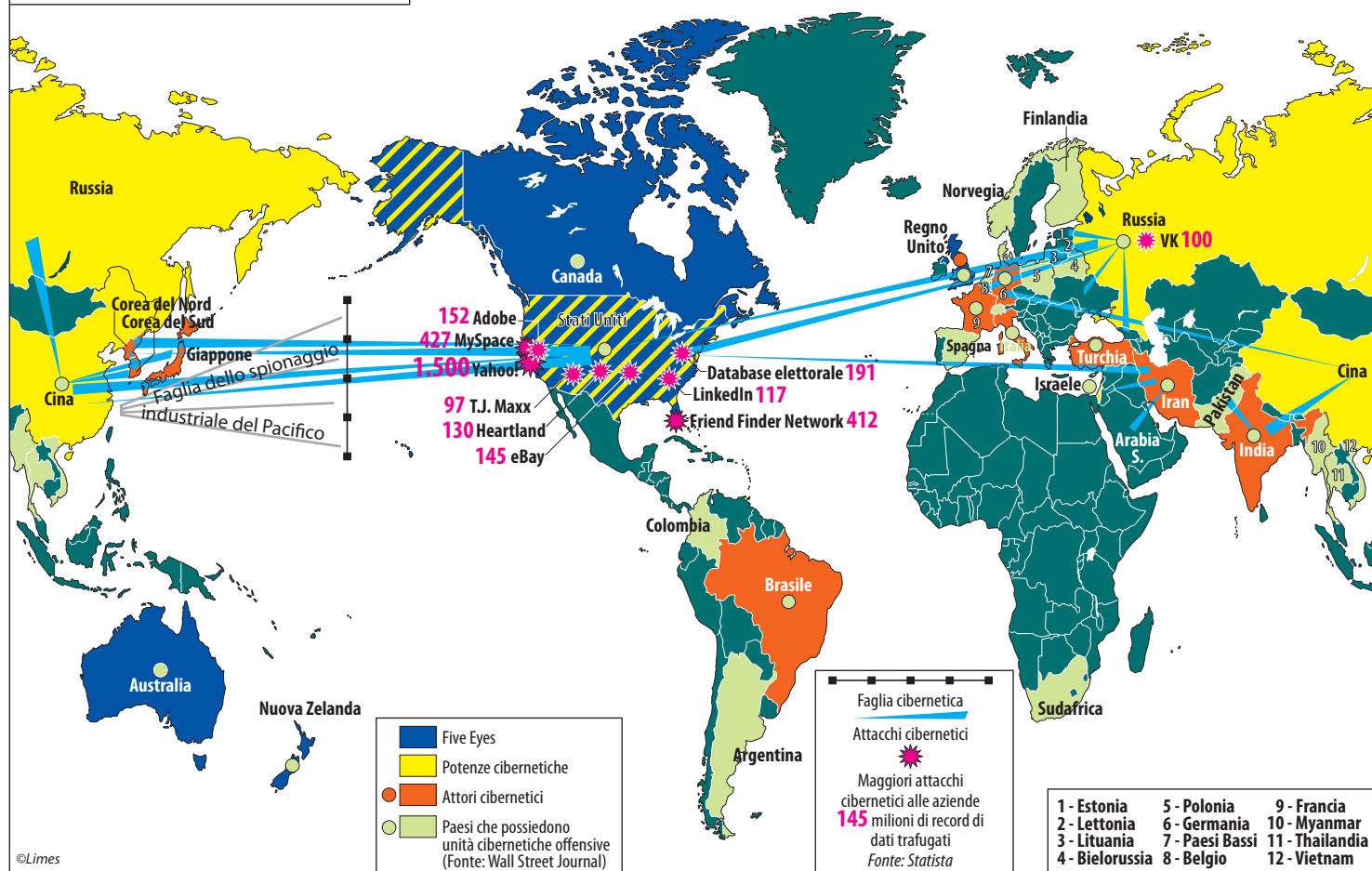
UN'ORA DI CIBERGUERRA

Tra le 14:45 e le 15:45 del 25 giugno 2014

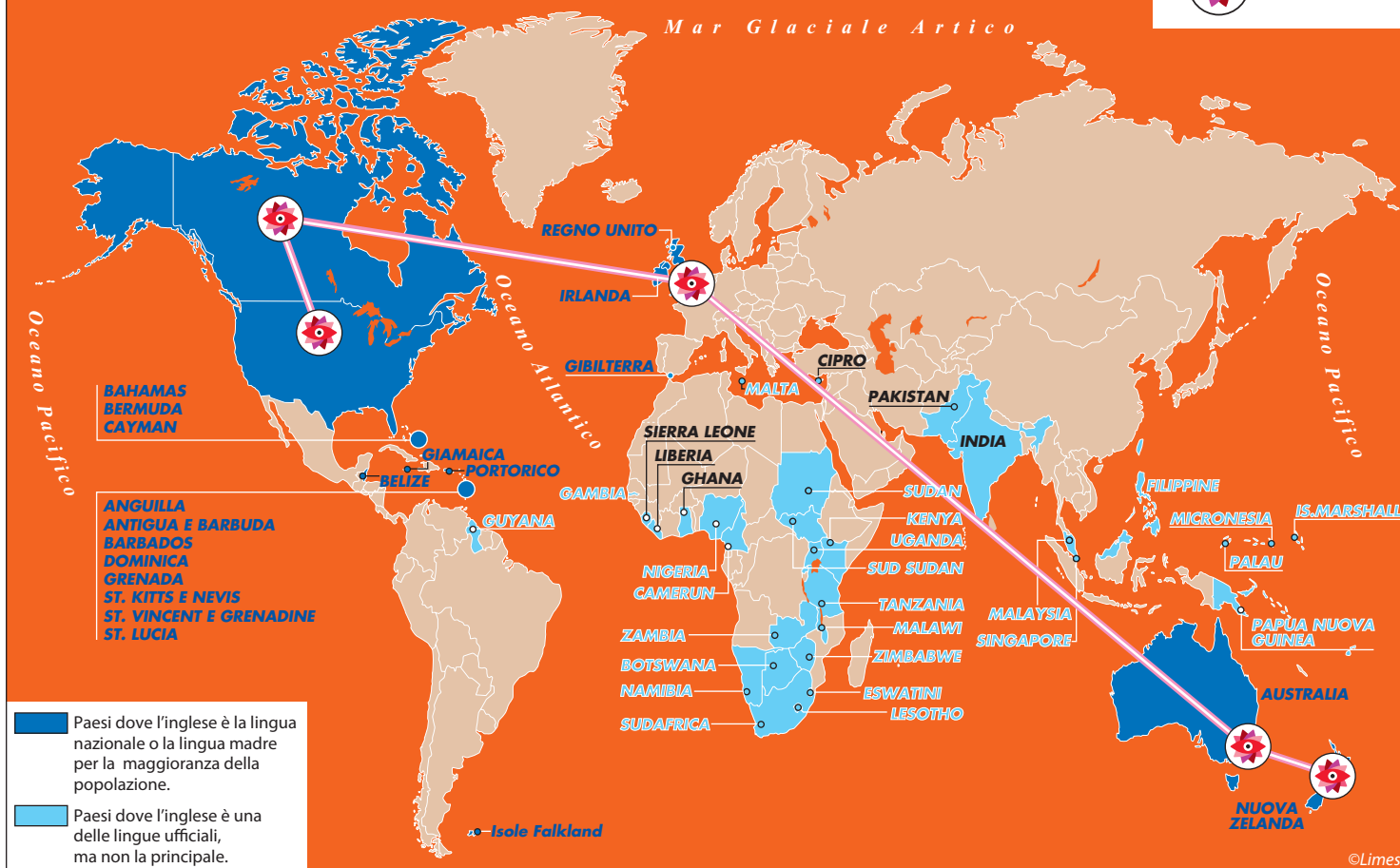


Fonte: Norse Corp.

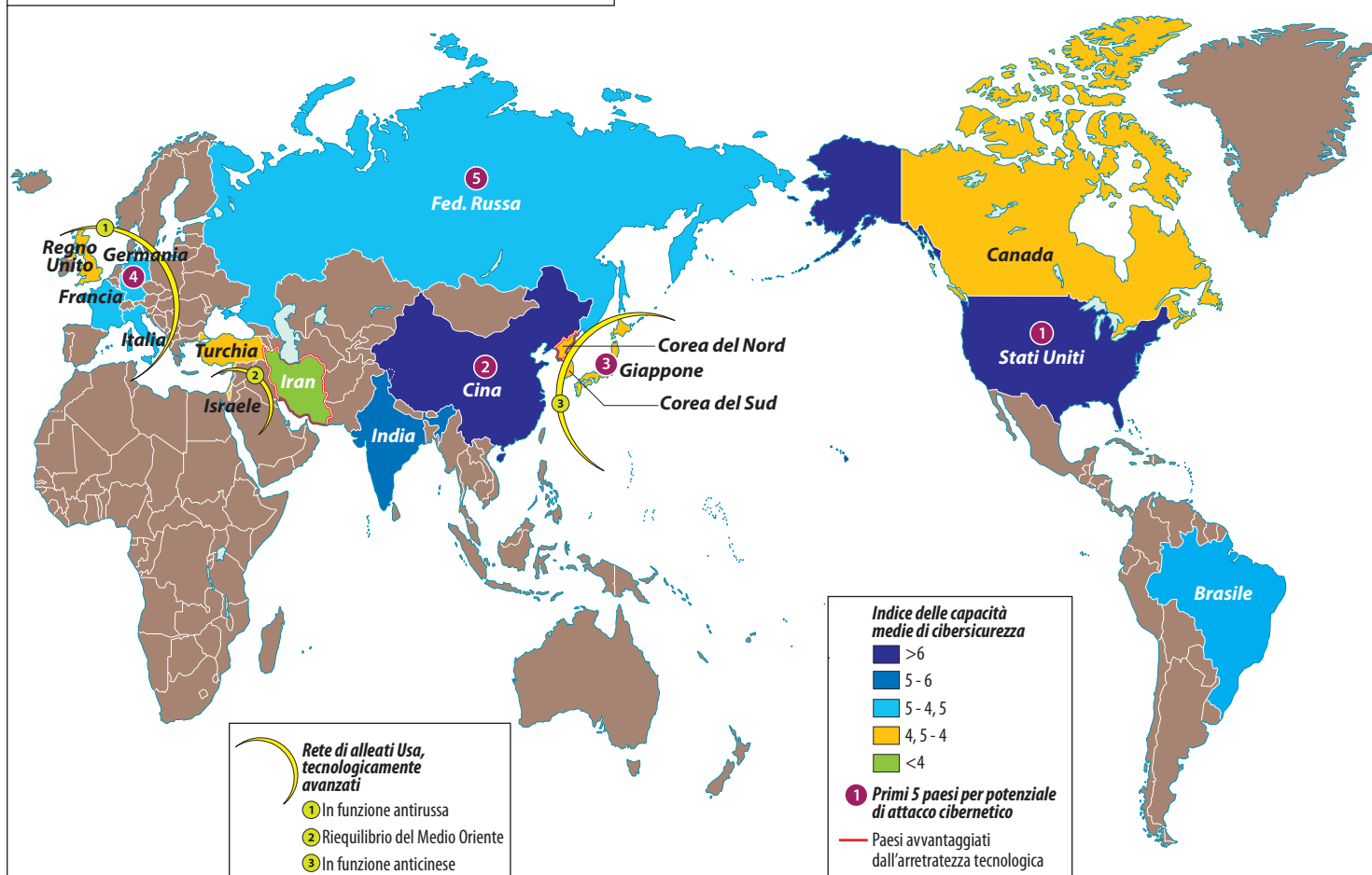
ATTACCHI CIBERNETICI



ANGLOSFERA



LE CAPACITÀ DELLE CIBERPOTENZE



Fonte: Università tecnica di Istanbul (Itu), 2018.

alla Difesa James Mattis a prevedere che «dovremo probabilmente offrire a banche, gestori di servizi pubblici e centrali elettriche l'opportunità di stare nella dimensione protetta dal governo»¹⁴. Le attività vitali per la sicurezza della nazione nella fortezza, il resto là fuori alla mercé dell'anarchia. S'intravede il rischio di erosione del monopolio sull'erogazione della sicurezza, il più prezioso degli attributi della statualità. Per conservarsi essenziale, lo Stato potrebbe un domani essere chiamato a iniettare una certa dose di protezionismo nei servizi fondamentali.

4. In questo scenario, sono gli stessi generali e funzionari d'intelligence statunitensi ad avvertire del rischio di puntare troppo sull'erigere difese in assenza di garanzie che funzionino. L'ex direttore dell'Nsa e primo capo del Comando cibernetico, generale Keith Alexander, amava agitare i precedenti della grande muraglia cinese e soprattutto della linea Maginot per marcare il punto. E per invocare più ampi poteri per andare all'attacco. Qui interviene il secondo fattore che rende il ciberspazio più competitivo: la cautela esibita sinora dagli Stati Uniti.

A ogni ciberattacco di una potenza avversaria, puntualmente la Casa Bianca promette rappresaglie proporzionali, da condurre nei tempi e nei modi che essa deciderà. Ma la risposta tarda a palesarsi. Potrebbe certo essere avvenuta sotto forma di intrusione e non essere stata ancora rilevata dal nemico. Oppure quest'ultimo, di fronte all'evidenza dell'attacco, potrebbe aver avuto tutto l'interesse a nascondere per non mostrarsi sguarnito. Gli Stati Uniti ne hanno senza dubbio la capacità. In passato, hanno penetrato le reti e i cavi sottomarini della cinese Huawei per spiare l'Esercito popolare di liberazione o pianificato di disconnettere completamente un paese (l'Iran, Operazione Nitro Zeus¹⁵). E hanno condotto operazioni cibernetiche conclamate contro lo Stato Islamico – benché con risultati molto deludenti, almeno stando al segretario alla Difesa dell'epoca, Ashton Carter¹⁶.

Eppure, a ogni quanto di sfida, la superpotenza tentenna. Non si mostra risoluta. «È un problema ricorrente», ammetteva il consigliere per la cibersicurezza del presidente Obama, Michael Daniels. «Nel momento in cui hai dichiarato chi c'è dietro un attacco cibernetico, la domanda successiva è: come fargliela pagare? E la risposta non sempre è facile»¹⁷. Dopo aver additato P'yŏngyang per l'attacco WannaCry, il consigliere per la sicurezza interna di Donald Trump, Thomas Bossert concedeva sull'orlo della sconsolazione: «Il presidente ha usato praticamente tutti gli strumenti disponibili, a parte affamare il popolo nordcoreano, per cambiare il loro comportamento»¹⁸.

La Corea del Nord è un caso molto peculiare, assai difficilmente replicabile visti l'estremo isolamento e l'arretratezza tecnologica che la rendono meno esposta

14. «Mattis Predicts DOD Will One Day Offer Cyber Protection to Private Sector», *Fifth Domain*, 27/9/2018.

15. D.E. SANGER, *op. cit.*, cap. 2.

16. A. CARTER, «A Lasting Defeat: The Campaign to Destroy ISIS», Belfer Center for Science and International Affairs, ottobre 2017.

17. D.E. SANGER, *op. cit.*, ed. Kindle, pos. 2413.

18. «Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea», White House, 19/12/2017.

alle rappresaglie americane – un modo ci sarebbe stato: passare attraverso le reti cinesi, ma Washington giustamente non era disposta a far temere a Pechino di essere sotto attacco. In ogni caso, la cautela non si limita al regime dei Kim. È la stessa riservata a lungo ai cinesi con il massiccio spionaggio industriale o ai russi con il sabotaggio delle elezioni del 2016. A spiegarla sono due ordini di ragioni.

Il primo riguarda la conoscenza ancora primitiva delle regole del gioco. Cos'è un attacco cibernetico? Che cosa differenzia un atto di ciberguerra da uno terroristico e da uno vandalico? Qual è la soglia tra criminalità individuale e sponsorizzazione statale? Come rispondere in modo proporzionale: limitarsi alla sfera digitale o distruggere entità fisiche? Quando bisogna difendere un'azienda e quando astenersi? È bene non sottovalutare questi dilemmi perché in essi sono rimaste confitte le amministrazioni americane da quando i rivali hanno iniziato a bersagliare il territorio nazionale, privandole della tradizionale sicurezza di confinare con paesi amici o con pesci. Soprattutto, questi interrogativi investono una tendenza alla compartimentazione con cui gli statunitensi si avvicinano alla competizione fra grandi potenze. Per anni, ad esempio, Obama e i suoi hanno provato a convincere la Cina a separare lo spionaggio per scopi di sicurezza nazionale (praticato anche dagli Stati Uniti, dunque buono) da quello industriale (praticato principalmente da Pechino, dunque cattivo). Lasciando piuttosto scettici gli interlocutori, per i quali il secondo ricade senza dubbio nel primo, in linea con la tendenza, non estranea nemmeno ai russi, a riconoscere valenza strategica a qualunque strumento sia impiegabile per acquisire un vantaggio sul rivale. L'unica distinzione che i cinesi praticano è quella fra spionaggio silenzioso e rumoroso – tant'è vero che dopo una piccola tregua sono tornati a trafugare senza sosta¹⁹.

La seconda ragione investe la segretezza che ammantava il mondo della ciberguerra, tipica di ciò che riguarda l'intelligence. L'Nsa è per costituzione restia a ogni pubblicità delle proprie capacità. Preme per non mostrare le prove del coinvolgimento di un attore statale nei ciberattacchi per tema di svelare come abbia fatto a ottenere le informazioni, cosa sappia delle operazioni avversarie e in quale punto della filiera nemica si sia collocata. Si oppone a impiegare le proprie armi in rappresaglie che le occluderanno l'accesso a sistemi già abbondantemente infiltrati. Basandosi sulle *backdoors*, le strategie di attacco sono di fatto usa e getta: una volta impiegate, le falle vengono individuate e chiuse. Ecco perché l'Nsa comunica alle aziende tecnologiche, da Apple a Microsoft, il 90% delle vulnerabilità dei software che passa in rassegna: il restante 10% lo conserva per sé. Quand'anche si decida di impiegare queste armi, spesso non è possibile stabilire in anticipo che effetto avranno. A meno di non colpire un singolo obiettivo – ma a quel punto che rappresaglia è? – il rischio è di fissare un pericolosissimo precedente iniettando in Rete un virus che si propaghi su dispositivi civili. Come peraltro già successo a Stuxnet, finito fuori controllo. Di lì a incescicare in un'escalation il passo è breve.

Anche perché un'altra consapevolezza caratterizza la mentalità dell'Nsa: quello che possiamo fare contro di loro può essere fatto contro di noi.

Nell'icastico riassunto dell'attuale capo dell'Nsa e del Comando cibernetico, generale Paul Nakasone, che nel marzo 2018, a un senatore che gli chiedeva che cosa succede ai ciberavversari dell'America quando la attaccano, rispondeva: «Direi che ora non pensano che gli accadrà granché. Non hanno paura di noi»²⁰.

5. Stabilito che cautela e squilibrio offesa-difesa limano le distanze fra attori cibernetici, come reagisce il Numero Uno? Nessuna delle alternative promette stabilità.

Si potrebbe pensare che il reciproco grado di penetrazione delle altrui reti imbastisca uno scenario simile alla mutua distruzione assicurata degli armamenti nucleari. In realtà, il paragone non tiene. Primo, le armi cibernetiche non seminano morte e distruzione con la stessa absolutezza, non sono arbitri del fato del pianeta. Secondo, e di conseguenza, vengono impiegate costantemente e per scopi meno apocalittici, dalla manipolazione psicologica alla coercizione, dallo spionaggio all'ostruzione delle operazioni rivali. Terzo, all'alba dell'età nucleare il dibattito strategico era acceso, pubblico, mentre ora un alone di mistero e confusione impedisce non solo ragionamenti ponderati, ma anche solo di sviluppare un deterrente credibile. «Non puoi fare di qualcosa che è segreto un deterrente, perché se non sai che c'è non ti fa paura», era l'inappuntabile logica dell'ex vicecapo degli Stati maggiori riuniti, generale James Cartwright²¹. Quarto, durante la guerra fredda attorno all'arma atomica erano proliferati trattati e norme informali di comportamento. Qui di regole neanche a parlarne. L'allora segretario alla Difesa Robert Gates aveva suggerito un incontro segreto con russi, cinesi, britannici, israeliani e francesi per stilare alcuni principi di massima, ma la proposta non è andata da nessuna parte²².

A questo proposito, si potrebbe concludere che un egemone responsabile sia tenuto a un solitario gesto di grande lungimiranza: prendere l'iniziativa e annunciare pubblicamente un codice di condotta cibernetico cui si atterrà il paese stesso e chi interessato a emularne l'esempio. Una mossa non del tutto disinteressata, argomenta chi la sostiene, poiché volta a sfruttare la finestra di superiorità prima che si chiuda del tutto. Eppure, assai difficilmente i successi della limitazione di altri tipi di armamenti funzionerebbero, anche in presenza di tanta nobiltà, poiché il progresso tecnologico procede talmente veloce da rendere obsoleto ogni tentativo in tal senso. Senza contare l'ovvia difficoltà di misurare la forza relativa dei vari attori e le violazioni²³. In ogni caso, la superpotenza non accetterebbe mai di diminuire il proprio rango sovraordinato rispetto agli altri, legandosi le mani già abbondantemente in pasta altrove. Come dimostra l'insurrezione al Pentagono del marzo

20. Audizione presso l'Armed Service Committee del Senato di conferma a comandante del Comando cibernetico degli Stati Uniti, 1/3/2018.

21. «Ex-U.S. General Urges Frank Talk on Cyber Weapons», *Reuters*, 26/11/2011.

22. Cfr. F. KAPLAN, *op. cit.*, pp. 272-73.

23. E.D. BORGHARD, S.W. LONERGAN, «Why Are There No Cyber Arms Control Agreements?», *Net Politics*, Council on Foreign Relations, 16/1/2018.

2013 contro il consigliere per la sicurezza nazionale di Obama, Tom Donilon, che si era scagliato contro l'attivismo cibernetico cinese sostenendo che «la comunità internazionale non si può permettere di tollerare qualunque attività di questo tipo da parte di qualunque paese»²⁴. Quei due *qualunque* includevano o no l'America? Nel dubbio, meglio evitare.

Non resta che passare all'offensiva. Sprovvisi di efficaci difese e in attesa dello sdoppiamento e della ridondanza di infrastrutture e sistemi d'arma per prevenirsi dalle reti già compromesse, gli Stati Uniti amplieranno l'uso delle capacità d'attacco. Diversi segnali nel 2018, soprattutto retorici, puntano in tal senso. A inizio anno, il Pentagono ha sottoposto alla Casa Bianca una strategia nucleare in cui si raccomandava di autorizzare l'uso dell'arma assoluta in caso di devastante ciberrat-tacco al paese²⁵. A maggio, il Cyber Command è stato elevato al rango di comando combattente e dopo nove anni di esistenza tutte e 133 le squadre operative hanno raggiunto la piena capacità (6.200 militari). Nella tarda estate, un memorandum presidenziale ha stralciato una precedente direttiva dell'amministrazione Obama che conferiva al solo comandante in capo l'autorità di ordinare operazioni dalle conseguenze significative (morti, possibili rappresaglie contro il paese, seri danni a entità fisiche). In base alla nuova politica, in determinate circostanze l'autorità è delegabile al segretario alla Difesa ed è allo studio di portarla ancora più in basso, al Comando cibernetico²⁶. Infine, il passaggio più rilevante della strategia cibernetica della Difesa pubblicata a settembre riguarda la «difesa avanzata» (*forward defense*) per «interrompere o fermare attività cibernetiche maligne alla fonte, incluse quelle al di sotto del livello di conflitto armato»²⁷. Tradotto: attacchi preventivi o, meglio, preservativi. Il più possibile dissimulati, ma pur sempre attacchi. Accettan-do l'anarchia e scommettendo che ciò che accade nel ciberspazio continui a restare nel ciberspazio. Nella consapevolezza (speranza?) che l'impero non cadrà per mano cibernetica. Per convincere gli avversari – e soprattutto sé stessa – di dispor-re ancora di una superiorità in questa dimensione hobbesiana, l'America sguaina la spada nelle aule cieche del Web.

24. Cfr. F. KAPLAN, *op. cit.*, pp. 226-27.

25. D.E. SANGER, W.L. BROAD, «Pentagon Suggests Countering Devastating Cyber Attacks with Nuclear Weapons», *The New York Times*, 16/1/2018.


26. D. VOLZ, «White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons», *The Wall Street Journal*, 20/9/2018.

27. «Summary: 2018 Department of Defense Cyber Strategy», U.S. Department of Defense, p. 1.

BOT RUSSI O AMERICANI PECORONI?

di Matthew CROSTON

Washington pensa di battere con contromisure poliziesche l'intrusività russa nei social media in America. Sbagliando: basterebbe diffondere un po' di pensiero critico. Mosca gioca sulla quasi impossibilità di provare le sue intrusioni.

1.  ALLE ELEZIONI PRESIDENZIALI DEL 2016, il governo, l'opinione pubblica e i media americani hanno un'ossessione fissa. Da quando gli inquirenti hanno accumulato sufficienti prove circostanziali dei tentativi russi di «influenzare» l'esito del voto, tutti cercano di capire non tanto come ciò sia stato possibile, quanto se questi sforzi abbiano interessato l'elezione di metà mandato del 2018 e soprattutto come Donald Trump imposterà la campagna per confermarsi alla Casa Bianca nel 2020.

Tutto ruota attorno alle due semplici virgolette apposte attorno al verbo «influenzare». Per quanto frustrante per analisti d'intelligence ed esperti accademici, la realtà è che è praticamente impossibile ottenere una prova definitiva (in senso legale) che le malefatte del 2016 siano state tali da rendere necessario invalidare i risultati delle urne. A illustrare la portata del problema bastino i modi cangianti con cui gli stessi americani hanno descritto gli sforzi avversari: cominciati come «dirette interferenze nelle elezioni», sono poi diventati «ovvie manipolazioni dei votanti», mentre ora si è passati all'ambigua e amorfa dicitura «probabile influenza maligna».

La domanda però è più ampia, raramente enfatizzata e tale da rendere questo dibattito del tutto irrilevante: come contrastare le misure attive russe, come le chiamano a Mosca, senza al contempo permettere al governo di aumentare il livello di invasività su Internet? Sarebbe sufficiente che una più critica opinione pubblica americana controllasse le informazioni che si leggono online, risalendo alla fonte. Sfortunatamente, pare che i cosiddetti esperti del settore abbiano più fiducia nell'intrusione tecnologica del governo che nell'intelligenza dell'elettorato americano. Ed è proprio questo fatto che potrebbe condurre la strategia cibernetica della Russia alla vittoria.

2. Mosca ha realizzato molto tempo fa che è nel suo miglior interesse impiegare capacità cibernetiche in aree in cui l'America può essere particolarmente

debole o vulnerabile. Lungi da chi scrive giustificare tale ragionamento strategico; tuttavia bisogna ammettere che la Russia considera apertamente da oltre due decenni le tecniche cibernetiche come una mera estensione di altri strumenti d'influenza. Non troppo distante dall'idea clausewitziana di guerra come prosecuzione della politica con altri mezzi. Per questa ragione, i russi giudicano ampollosi gli intensi dibattiti in Occidente se considerare lo spazio cibernetico una nuova dimensione bellica o creare nuove norme internazionali per governare il comportamento degli Stati in questa sfera. Il Cremlino ritiene la cibernetica semplicemente uno strumento che lo Stato adopera per acquisire un vantaggio e proteggere gli interessi nazionali. Giusto o sbagliato che sia, ha solamente preso la decisione che l'uso strategico dei social network negli Stati Uniti è un elemento indicativo e normale di questa filosofia.

Le manovre sono iniziate molto prima del voto del 2016 con le goffe intrusioni nei server del Comitato nazionale democratico, ma in seguito si sono evolute in un impiego più sofisticato di Facebook, Twitter, Instagram eccetera. Gli operatori russi hanno usato le *virtual private networks* (vpns) per dotarsi di autentici indirizzi Ip statunitensi. Le operazioni erano condotte in orari in cui veri utenti americani si sarebbero collegati a Internet. Esseri umani in carne e ossa sono stati impiegati quantomeno per replicare lo stile narrativo, linguistico e comportamentale dei bersagli. Sono stati sfruttati conti correnti in banche americane per acquistare spazi pubblicitari sulle piattaforme social. Non si sono fatti mancare furti d'identità per condire il tutto con una spruzzata di verosimiglianza.

In questo modo, le operazioni che inizialmente lasciavano qualche traccia si sono talmente complicate e ramificate da rendere il compito degli inquirenti paragonabile a quello di andare a cercare le prove in infinite tane di Bianconiglio. Francamente, i rozzi hackeraggi della posta elettronica dei democratici erano molto in odore di abc dello spionaggio della guerra fredda. Tuttavia, i russi hanno imparato due lezioni più velocemente degli americani. Primo, è molto difficile ottenere con questi sotterfugi una «pistola fumante» per compromettere definitivamente un candidato. Secondo, non appena si scopre che c'è una potenza straniera dietro questo tentativo di diffamare un individuo specifico la reazione dell'opinione pubblica vira comprensibilmente verso il patriottismo. Così, i russi sono passati a un piano che negli Stati Uniti è stato descritto come tentativo di «inficiare la democrazia e diffondere discordia sociale».

Gli sforzi in tal senso sono così numerosi e ramificati da non poter essere riassunti qui. Tuttavia, il loro minimo comun denominatore era favorire lo sviluppo di posizioni estreme sui social media a entrambi i capi dello spettro politico americano. Negli Stati Uniti, tali pervicaci e devianti pratiche sono state bollate come particolarmente efficaci, anche se finora non si è riusciti a dimostrarne i risultati concreti. Al di là di ciò, gli americani hanno preso la sfida cibernetica russa alla democrazia con estrema serietà. Si è scomodata nientemeno che un'autorità come James Stavridis, già comandante della Nato e a capo dell'influente Fletcher School

alla Tufts University, per suggerire quattro specifici metodi con cui contrastare la guerra mediatica di Mosca¹.

A) Migliore cooperazione pubblico-privata: i social media come Facebook e Twitter dovrebbero ospitare personale di collegamento dell'Nsa, della Cia o dell'Fbi per facilitare la comunicazione e il coordinamento in caso di intrusioni simili.

B) Migliori difese tecniche: l'America deve sviluppare superiori strumenti di indagine per identificare i bot e altre cibertecnologie dannose in tempo reale e deve adeguare in tal senso le proprie strategie di difesa.

C) Migliore pubblicità: bisogna potenziare sensibilmente la capacità di rivelare l'identità, la natura e l'estensione di questi ciberattacchi. Fare ciò agevola di conseguenza gli Stati Uniti nel tentativo di ridurre l'impatto di tali operazioni.

D) Combattere per sé stessi: gli Stati Uniti devono essere più aggressivi, anche in pubblico, nel rispondere agli attacchi. È una questione di deterrenza: se la controparte ha buone ragioni di temere ripercussioni, forse desisterà dal proseguire le incursioni.

Questi saggi investimenti nella ciberdeterrenza di lungo periodo non hanno nulla di sbagliato. Tuttavia, appare chiaro come la mentalità poliziesca della vecchia scuola non serva a granché per fermare la minaccia. Un esempio lampante proviene dai 13 membri della comunità dell'intelligence russa iscritti al registro degli indagati dal dipartimento di Giustizia. Queste stesse persone continuano a vivere e lavorare tranquillamente in patria e il Cremlino si è limitato a negare la possibilità di estradarle, quand'anche gli Stati Uniti lo richiedessero – Washington non lo ha nemmeno fatto. Casi come questo ricadono nella sfera simbolica: servono a trasmettere ai cittadini la sensazione che il governo si stia occupando della faccenda quando invece mosse retoriche del genere non hanno alcuna ricaduta pratica.

3. La maggior parte delle analisi che provano a suggerire contromisure alle operazioni cibernetiche e mediatiche russe possiede un tratto comune: il totale rifiuto di accettare responsabilità pubbliche e intellettuali. Prendiamo un esempio concreto. Su Facebook, gli operatori russi hanno pubblicato una notizia secondo la quale due gruppi politici di visioni diametralmente opposte intendevano tenere le rispettive manifestazioni nello stesso luogo di una città del Texas alla stessa ora dello stesso giorno. Si trattava di un'organizzazione dichiaratamente anti-immigrazione e islamofoba e di un'altra invece aperta agli immigrati e promotrice di una «migliore comprensione» della religione maomettana. La notizia ha comprensibilmente scatenato accesi scontri sullo stesso Facebook tra veri utenti texani, che si sono propagati in modo virale fino a spingere molti a pensare di trovarsi nell'imminenza di una specie di guerra civile. L'unico problema è che nessuno aveva alcuna intenzione di manifestare in Texas quel giorno. Peggio, i due gruppi nemmeno esistevano.

1. J. STAVRIDIS, «Four Ways to Counter Russia's Social-Media Warfare», *Bloomberg*, 7/8/2018.

Si tratta senza dubbio di un uso irresponsabile e potenzialmente pericoloso di Internet per scopi riprovevoli. Ma mi lascia sempre basito che nessuno in America sembri concentrarsi sull'unica soluzione in grado di eliminare davvero il problema: educare l'opinione pubblica – fino a inculcarglielo in testa – a un sano scetticismo che spinga ad andarsi a cercare le informazioni su varie fonti invece di affidarsi a una sola. Un tempo questa semplice tecnica la si impartiva ai primi anni della scuola superiore per insegnare a pensare in modo analitico e a sostenere le proprie idee con solide argomentazioni. Ora invece sembra di chiedere troppo agli adulti là fuori, che dovrebbero essere pienamente consapevoli non solo delle proprie libertà civili ma pure delle proprie responsabilità civiche. Nell'esempio di prima, sarebbe stato sufficiente battere qualche tasto in più per chiedere a Google: «Ci sono gruppi islamici e anti-islamici che manifestano in Texas oggi?». La ricerca avrebbe rivelato la fandonia e avrebbe spento sul nascere non solo la crisi, ma anche ogni timore che una nazione avversaria stesse cercando di seminare zizzania.

La stessa, semplice strategia sarebbe stata opportuna pure con una delle più famose misure attive russe in vista delle elezioni del 2016, ovviamente diventata virale e diffusa da migliaia di utenti americani: la «Killary list». I siti Web che hanno diffuso la notizia pretendevano di «provare» che una cinquantina scarsa di persone era morta o si era suicidata in circostanze sospette poco prima di testimoniare contro presunte pratiche corrotte o illegali di Hillary Clinton. L'unica cosa più irrazionale e inspiegabile della bufala stessa è come a essa abbiano abboccato tanti rispettabili conservatori americani fino a diffonderla sui propri profili social. Servono letteralmente pochi movimenti delle dita su una tastiera per accertarsi che l'allora candidata alla presidenza non era affatto indagata e che il governo degli Stati Uniti non aveva guardato dall'altra parte mentre una spietata serial killer si rendeva responsabile della morte di più di quaranta persone.

Eppure, ancora oggi, Washington sembra più intenta a dotarsi di misure di ciberdeterrenza che verranno superate sei mesi dopo essere entrate in vigore (o anche solo proposte). Peraltro, per svilupparle, occorrerà forgiare una scomoda alleanza fra il settore privato e quello pubblico che garantirà all'establishment dell'intelligence accesso a documenti e informazioni aziendali sino a quel momento confidenziali.

4. Oggi le maggiori preoccupazioni, visto chi occupa la Casa Bianca e le possibili influenze della Russia sul presidente, si concentrano su un'eventuale mancanza di leadership nella difesa della popolazione. Non è certo appropriato né moralmente giusto che una nazione straniera causi impunemente disagi e disordini sociali al di fuori dei propri confini. Ma è curioso che in questo dibattito nessuno si faccia domande sulla leadership che ognuno di noi dovrebbe esercitare: che ruolo ha il popolo americano nel proteggere le proprie menti e convinzioni? Alla fine della fiera, la malignità dell'altrui influenza investe la sfera personale.

E come tale ogni individuo la può controllare.

Non auspico certo di vedere i social media sopraffatti dai bot della Russia o di qualunque altra nazione, Stati Uniti compresi. Ma l'unico vero pericolo di queste tecnologie è che vengano in contatto con un popolo di pecoroni²: individui facilmente manipolabili perché non interessati al pensiero analitico, a fare ricerche per conto proprio o a commenti sostenuti dai fatti. Se alla fine gli unici contenuti politici a cui gli americani vogliono essere esposti sono notizie che confermano le loro convinzioni e l'odiosità dei loro oppositori, allora raccoglieranno sempre ciò che avranno pigramente seminato.

In tal caso, per riconoscere il nemico sarà sufficiente guardarsi allo specchio. Non ci vedremo dei bot russi. Ma dei pecoroni.

(traduzione di Federico Petroni)

2. In originale, *sheeple*, crasi fra *sheep* (pecora) e *people* (popolo), *n.d.t.*

IL PIANO DI XI JINPING PER SUPERARE GLI USA NELL'INTELLIGENZA ARTIFICIALE

Il divario tra le due potenze nell'Ai si assottiglia, ma Pechino resta indietro. L'unione tra industria militare e civile cinese rivela uno scopo volto al controllo della popolazione, non solo bellico. Una misteriosa microspia inquieta gli americani.

di Giorgio CUSCITO

LA CINA È PER MOLTI VERSI GIÀ UNA potenza nel campo dell'intelligenza artificiale (Ai) e punta ora a sorpassare gli Stati Uniti. Pechino sta compiendo grandi sforzi per valorizzare lo sviluppo di nuove tecnologie, software e processi utili a rendere più efficiente l'economia cinese e a migliorare le capacità dell'Esercito popolare di liberazione (Epl) nelle guerre future.

Sul piano qualitativo, la Repubblica Popolare ha ancora qualche lacuna, ma sta rapidamente colmando il divario con gli Usa grazie al forte sostegno governativo alle aziende tecnologiche nazionali, alla grande quantità di metadati a disposizione e al fermento dell'imprenditoria cinese. Anche per questo, Washington punta a ostacolare il percorso di crescita tecnologica della Repubblica Popolare, di cui il progetto Made in China 2025 è la colonna portante.

Il piano di Pechino

La Repubblica Popolare vuole diventare un centro globale per l'innovazione nel campo dell'Ai entro il 2030, secondo il Piano di sviluppo per la nuova generazione dell'intelligenza artificiale annunciato lo scorso anno¹. Oggi in Cina questo settore vale 3,5 miliardi di dollari. Fra 12 anni la cifra ammonterà a 150 miliardi, secondo le stime di Pechino. Il ministero della Scienza e della Tecnologia cinese ha assegnato a cinque aziende il compito di accelerare lo sviluppo dell'Ai: Baidu, Alibaba, Tencent (concorrenti delle statunitensi Google, Amazon e Facebook),

1. Guowuyuan guanyu yinfaxin yidai rengong zhineng fazhan guibua de tongzhi (Comunicato del Consiglio di Stato sulla pubblicazione del piano di sviluppo della nuova generazione d'intelligenza artificiale), gov.cn, 8/7/2017, goo.gl/hSFHft

iFlytek e SenseTime. La prima si occuperà del progresso della guida autonoma, tramite il progetto Apollo. In questo campo, Baidu peraltro collabora con la tedesca Daimler, che possiede Mercedes-Benz. Alibaba dovrà ottimizzare il sistema di trasporto urbano. Tencent (che possiede WeChat) dovrà esplorare l'utilizzo dell'AI per le diagnosi mediche. Inoltre, l'azienda ha annunciato una grande opera di ristrutturazione e la creazione di due nuovi dipartimenti focalizzati sulle attività *cloud* e lo sviluppo di piattaforme Web. iFlytek si focalizzerà sul riconoscimento vocale, settore in cui è all'avanguardia, e creerà il primo laboratorio cinese per il calcolo cognitivo, per affinare le capacità di ragionamento e comprensione dei computer. SenseTime si concentrerà invece sullo sviluppo del riconoscimento di volti e immagini. La chiara suddivisione dei compiti stabilita da Pechino collima con i suoi obiettivi geopolitici di lungo periodo.

Crescita e monitoraggio

Sul fronte domestico, due scopi guidano lo sviluppo dell'intelligenza artificiale in Cina: crescita economica e stabilità interna (*weiwén*). L'AI può rendere efficienti le attività nei settori più disparati: salute, istruzione, finanza, trasporti, tutela ambientale, guerra, cibersicurezza, lotta alla criminalità, antiterrorismo, controllo della popolazione, prevenzione di disordini sociali. In sintesi, il balzo tecnologico può alimentare lo sviluppo del paese lungo il percorso di «risorgimento» della nazione annunciato dal presidente cinese Xi Jinping. Questo processo, che dovrebbe completarsi entro il 2049, implica grandi sfide socio-economiche, come la riduzione della dipendenza dalle esportazioni, la diminuzione del divario di ricchezza coste/interno, città/campagne, e l'aumento dei consumi interni. Le riforme che Xi vuole sviluppare (inclusa quella delle imprese di Stato) potrebbero alimentare nuove tensioni interne. Di qui la necessità di elevare il livello di monitoraggio della popolazione cinese, che oggi ammonta a 1,4 miliardi di abitanti.

Sono 170 milioni le telecamere di sorveglianza presenti nel paese. In 16 province, Pechino già usa il sistema Sky Net, che si serve del riconoscimento facciale per controllare la popolazione. Secondo i media cinesi, il programma scannerizza i volti in un solo secondo, ha un'accuratezza del 99,8% e negli ultimi due anni avrebbe permesso l'arresto di oltre duemila latitanti². Durante una simulazione condotta dalla polizia del Guiyang (nel Guizhou) in collaborazione con la Bbc, la tecnologia cinese ha impiegato solo sette secondi per individuare il corrispondente della testata britannica mentre si aggirava per la città. Le forze dell'ordine disponevano esclusivamente della sua foto. In alcune località della Cina, inclusa Pechino, la polizia sta anche testando occhiali dotati di intelligenza artificiale, che forniscono dati in tempo reale sui soggetti inquadrati nell'obiettivo. Le capacità cinesi nel campo del riconoscimento facciale sono state riconosciute anche dagli Usa. Per

esempio, nel novembre 2017 la start-up cinese Yitu si è classificata prima in una gara allestita dall'Intelligence Advanced Research Project Activity (Iarpa), che fa capo all'ufficio del direttore dell'intelligence nazionale a stelle e strisce.

L'intelligenza artificiale sarà utile anche allo sviluppo del sistema di credito sociale. Il meccanismo di valutazione comportamentale che sarà attuato a livello nazionale nel 2020 prevede premi e sanzioni alla popolazione ed è basato su una capillare raccolta dati su individui, imprese ed enti governativi. L'obiettivo è digitalizzare le già esistenti forme di controllo e indurre i cittadini al rispetto della legge.

Alibaba e Tencent sono state incaricate dal governo cinese di sviluppare un proprio sistema di credito sociale, a cui gli utenti possono sottoporsi volontariamente (a differenza di quello pubblico di futura applicazione) per ottenere dei premi in base ai pagamenti realizzati online, alla rete di contatti e al comportamento sul Web. Se il punteggio complessivo è alto, si ottengono degli sconti o delle agevolazioni sull'acquisto di prodotti. Non vi sono ripercussioni di natura legale in caso di punteggi bassi, a differenza invece di quanto accade con il credito sociale pubblico. L'obiettivo del meccanismo realizzato da Tencent e Alibaba è integrare nel sistema di credito finanziario nazionale i cittadini che non hanno mai condotto transazioni bancarie. La raccolta di queste informazioni consentirà alle imprese tecnologiche e allo Stato di sviluppare gli algoritmi utili allo sviluppo dell'intelligenza artificiale.

Dal weiqi alla 'rivoluzione militare'

Le potenzialità dell'Ai in campo militare sono balzate agli occhi della Cina solo da qualche anno. In particolare, l'Epl ne ha compreso realmente la rilevanza dopo che il software Alphago di Google DeepMind Lab ha sconfitto il sudcoreano Lee Sedol nel 2016 e il cinese Ke Jie l'anno dopo nel millenario *weiqi* (o *go*). Il «gioco dell'accerchiamento» (questo significa *weiqi*), uno dei più complessi al mondo, è un esempio del pensiero strategico cinese. L'obiettivo è accerchiare con le proprie pedine (tutte di uguale valore) quelle dell'avversario su una griglia 19x19. La partita rappresenta una campagna prolungata, non una battaglia decisiva come negli scacchi. Il numero delle mosse possibili è superiore a quello degli atomi stimati nell'universo visibile. Dalla prospettiva dell'Epl, le vittorie della macchina sull'uomo nel *weiqi* hanno rappresentato una sorta di epifania: indicano che le potenzialità dell'Ai in campo militare sono sconfinite. Sul piano tattico e strategico. Al punto che dal 2016 in poi si sono svolte diverse conferenze di alto livello su questo argomento, a cui hanno partecipato anche esponenti della Commissione militare centrale (Cmc), l'organo supremo di comando delle Forze armate.

L'Epl vuole passare dalla guerra «informatizzata» (basata sulla circolazione potenziata e costante delle informazioni) a quella che prevede l'utilizzo dell'Ai, dei big data e delle tecnologie *cloud* in tutti gli aspetti della guerra. Incluse quelle di comando e controllo e lo sviluppo delle operazioni militari congiunte tra le varie branche militari delle Forze armate. I cinesi indicano la seconda fase con il termine

zhineng hua, che gli inglesi traducono approssimativamente con *intelligentized*. Questo processo determinerà una profonda «rivoluzione militare» (*junshi geming*) a detta di Liu Guozhi, capo della commissione per la Scienza e la Tecnologia della Commissione militare centrale.

I progressi delle aziende private tornano utili anche alle Forze armate. Per questo, nel 2017 Xi Jinping ha istituito un comitato per la «fusione» tra industria militare e civile (*junmin ronghe*). Curiosamente, i media cinesi traducono *ronghe* con l'inglese *integration*, forse per smussare agli occhi stranieri l'impatto del sostegno reciproco tra i due settori. All'interno della sopramenzionata commissione è stato istituito un centro d'innovazione congiunto per la cibersicurezza, che ha il compito di migliorare la qualità dei sistemi difensivi dell'Epl. L'intelligenza artificiale può ottimizzare l'addestramento del personale militare (quello cinese ha poca esperienza di combattimento reale), l'utilizzo degli «sciame» di droni, la capacità dei missili di individuare e colpire i bersagli, diagnosticare vulnerabilità proprie e altrui nel ciber spazio e rendere più rapida l'analisi di intelligence.

L'approccio dell'Epl all'intelligenza artificiale è ancora in fase di definizione. Le sue potenzialità potrebbero indurre le Forze armate a concentrare l'attività umana nell'ambito della supervisione, riducendo al minimo la presenza sul campo di battaglia. L'Ai potrebbe anche essere utilizzata come strumento per accentrare ulteriormente il processo decisionale all'interno dell'Epl e consentire ai vertici militari di prendere non solo decisioni strategiche, ma anche di aggirare la catena burocratica per avere un impatto diretto su quelle tattiche³. La più grande controindicazione alla base di una simile dinamica è che le macchine - come gli uomini - possono sbagliare. Se l'algoritmo che guida il missile è errato, questo può scambiare un bersaglio civile per uno militare. Motivo per cui Liu Guozhi ipotizza una crescente integrazione tra il pensiero umano e l'intelligenza artificiale, anziché la sostituzione del primo con la seconda, per potenziare il processo decisionale. Questa «simbiosi» richiederà personale altamente qualificato. Ma la Cina non ha ancora un così ampio bacino di talenti cui attingere.

Punti di forza e lacune della Cina

Diversi studi sostengono che la Cina deve ancora fare molta strada per colmare il gap con gli Usa nello sviluppo dell'intelligenza artificiale. Secondo un rapporto dell'Università di Oxford, su un indice di potenziale nell'Ai che va da 0 a 100 la Cina ha totalizzato 17 punti, mentre gli Usa ne hanno ottenuti 33⁴.

È lecito pensare che nei prossimi anni questo divario sia ridotto. La Cina ha due vantaggi. Il primo è che le aziende del settore godono del massiccio appoggio finanziario offerto dal governo per sviluppare e comprare nuove tecnologie e attrarre finanziamenti stranieri. Secondo un rapporto dell'Università Tsinghua di Pechino, tra

3. Cfr. E.B. KANIA, «Quest for an AI Revolution Warfare», *Real Clear Defense*, 8/6/2017.

4. Cfr. J. DING, «Deciphering China's AI Dream», University of Oxford, marzo 2018, goo.gl/SMBQks

il 2013 e il 2018 la Repubblica Popolare ha attirato il 60% degli investimenti elargiti a livello globale nel campo dell'Ai⁵. A ottobre, la China Development Bank ha finanziato lo sviluppo digitale con 14,55 miliardi di dollari. Il governo cinese ha investito 2,3 miliardi di dollari in un centro di ricerca per l'Ai a Pechino e altri 5 miliardi per uno a Tianjin.

Il secondo vantaggio delle aziende tecnologiche della Repubblica Popolare è l'accesso al più grande bacino di utenti Internet al mondo, da cui estrarre metadati e sviluppare algoritmi. Le potenzialità dell'economia digitale cinese sono incredibili. Oggi in Cina 800 milioni di persone navigano nel Web: più del doppio della popolazione statunitense, ma solo il 60% degli abitanti della Repubblica Popolare⁶. Ciò significa che l'economia digitale del Dragone, che vale quasi 4 mila miliardi di dollari, deve ancora sprigionare tutte le sue potenzialità. Imprese statunitensi come Apple, Google e Facebook lo sanno e per questo paiono disposte a piegarsi alla «sovranità cibernetica» cinese pur di fare affari.

Una delle carenze della Repubblica Popolare rispetto agli Usa è il numero inferiore di start-up impiegate nell'Ai. Uno studio delle società tedesche Roland Berger e Asgard Capital sostiene che la Cina ne conta 383 (l'11% del totale a livello mondiale), mentre gli Stati Uniti ne hanno ben 1.393⁷. I 2,6 miliardi di dollari incassati dalle imprese cinesi tra il 2012 e il 2016 sono pochi rispetto ai 17,9 miliardi incamerati dalle concorrenti a stelle e strisce. Tuttavia, la combinazione tra capitali provenienti dall'estero, effervescenza dell'imprenditoria nazionale e supporto di Pechino stanno alimentando la crescita del settore privato del Dragone. Sensetime è la start-up con la più alta valutazione al mondo, tre miliardi di dollari. La Microsoft Research Asia, fondata dal guru del settore Kai-Fu Lee, ha invece formato cinquemila esperti di Ai, che poi sono entrati in altre aziende e università della Repubblica Popolare. Anche Foxconn, (produttrice di componenti elettronici per aziende come Amazon, Apple e Microsoft) investirà almeno 342 milioni di dollari in cinque anni per assumere talenti nel campo dell'intelligenza artificiale e ottimizzare così l'attività manifatturiera.

Non bisogna sottovalutare inoltre l'interesse riscosso all'estero dalla tecnologia cinese, in particolare quello dei paesi che ricercano prodotti ad alto contenuto

LE PAROLE CHIAVE DELL'INTELLIGENZA ARTIFICIALE IN CINA

人工智能 (rengong zhineng):	intelligenza artificiale
信息化 (xinxihua):	informatizzazione
维稳 (weiwen):	mantenere la stabilità sociale
智能化 (zhinenghua):	uso dell'intelligenza artificiale in tutti gli aspetti della guerra
军民融合 (junmin ronghe):	fusione militare-civile
网络安全 (wangluo anquan):	cybersecurity
网络强国 (wangluo qiangguo):	potenza cibernetica
万维网 (wanweiwang):	World Wide Web o "www"

5. «Zhongguo rengong zhineng fazhan baogao 2018» fabu (Pubblicato il «Rapporto 2018 sullo sviluppo dell'intelligenza artificiale cinese»), Beijing, Università Tsinghua, 17/7/2017.

6. Di 42 ci «Zhongguo bulin wangluo fazhan zhuangkuang tongji baogao» fabu (Pubblicato il quarantaduesimo «Rapporto statistico sullo sviluppo della rete Internet in Cina»), China Internet Network Information Center, 20/8/2018, goo.gl/bUanW2

7. «Artificial Intelligence – A Strategy for European Startups: Recommendations for Policymakers», Asgard and Roland Berger, maggio 2018, goo.gl/XsnHyk

tecnologico a prezzi contenuti. Lo Zimbabwe, per esempio, ha siglato un accordo con l'impresa cinese CloudWalk, specializzata nel riconoscimento facciale. L'azienda non esporterà i suoi prodotti solo per aumentare i profitti, ma anche per sviluppare software in grado di elaborare i dati biometrici degli africani. In questo modo eleverà la capacità di monitoraggio nel Continente Nero, dove la Repubblica Popolare ha ormai solidi interessi economici e militari.

Un'altra differenza tra le prime due potenze al mondo si registra sul fronte della ricerca accademica. Quella cinese ha prodotto più articoli di quella statunitense sull'intelligenza artificiale, ma gli studiosi della Repubblica Popolare impiegati nel settore sono solo 18.232, il 9% del totale a livello mondiale ma il 5% in meno rispetto agli Usa. Soprattutto, i «talenti» cinesi sarebbero solo un quinto di quelli statunitensi⁸. Per accrescere il bacino di ricercatori, Pechino ha avviato un programma per incoraggiare i migliori a restare in patria, mentre alcune aziende cinesi hanno aperto proprie accademie per l'AI all'estero per reclutare quelli stranieri. La Repubblica Popolare è seconda agli Usa anche in termini di capacità innovative. Infatti produce meno brevetti nel campo dell'intelligenza artificiale rispetto alla diretta concorrente.

La Cina è infine carente anche nel settore hardware, nel quale impiega solo settecento aziende. Gli Usa ne contano quasi tremila. Lo sviluppo dei processori e dei chip richiede costi iniziali elevati e un lungo ciclo di creazione. Nel 2015, la Cina ha prodotto solo il 4% dei semiconduttori su scala mondiale, gli Usa ne hanno fabbricato il 50%. In sostanza, il Dragone in questo campo dipende ancora dall'importazione e dall'acquisizione di aziende straniere. Alla luce anche del più attento monitoraggio statunitense ed europeo verso le imprese cinesi, al momento questa mancanza è per Pechino la più difficile da sanare⁹.

Dietro il velo della guerra commerciale

Gli Stati Uniti riconoscono i rapidi progressi registrati dalla Repubblica Popolare. La guerra commerciale mossa da Trump cela infatti il tentativo di arginare nel medio periodo l'ascesa tecnologica cinese. Nel solo mese di ottobre, tre eventi hanno confermato questa dinamica. Il Pentagono ha accusato la Cina di mettere a rischio il complesso industriale militare degli Usa, di cui controllerebbe in parte la fornitura di tecnologia e materiale essenziale. La Repubblica Popolare possiede per esempio la maggior quantità al mondo di terre rare, elementi chimici che servono a fabbricare prodotti ad alto contenuto tecnologico. Il Tesoro Usa ha annunciato che potrebbe elevare il livello di controllo nei confronti degli investimenti stranieri, a cominciare proprio da quelli della Cina. Infine, *Bloomberg* ha divulgato una discussa inchiesta sull'hackeraggio cinese. Secondo la testata, l'intelligence dell'Epl avrebbe inserito dei chip piccoli come un chicco di riso in componenti elettronici costruiti in Cina per conto dell'azienda statunitense Super-

8. Si veda la nota 5.

9. Si veda J. DING, *op. cit.*

micro, che vende i suoi prodotti ad Apple, Amazon, Cia e Pentagono. La tecnologia innestata servirebbe per spiare le loro attività. I due colossi dell'economia statunitense e la stessa Supermicro hanno smentito. Quindi, o *Bloomberg* si sbaglia oppure i diretti interessati mentono, per paura di compromettere i rapporti con i consumatori e con la Cina.

A prescindere dalla fondatezza dell'inchiesta, Washington vuole screditare la filiera produttiva cinese per slegarla dalla propria. Impedendo così il trasferimento di conoscenza tecnologica, legale o illegale. Si tratta di un processo complesso da portare a termine, visto che la Cina svolge ancora un ruolo essenziale nella filiera tecnologico-produttiva statunitense e mondiale. Inoltre, le aziende Usa non intendono rinunciare ai vantaggi dell'accesso al mercato digitale cinese. Tencent ha un proprio centro per l'AI a Seattle. Google ne ha uno a Pechino (l'unico in Asia) e sta producendo una nuova versione del motore di ricerca ad hoc per la Cina, monitorato e censurato da Pechino. Nel 2018, Apple ha invece spostato le chiavi di accesso degli account iCloud cinesi all'interno della Repubblica Popolare, sottoponendo di fatto i loro traffici alla supervisione cinese. Anche la Tesla, gigante Usa specializzato nella produzione di veicoli elettrici, ha annunciato che costruirà la sua prima fabbrica all'estero nella Repubblica Popolare. Il trasferimento di conoscenza tecnologica che deriva da queste collaborazioni potrebbe favorire il già rapido piano di sviluppo dell'AI attuato da Pechino.

INTERVISTA

‘In Cina, WeChat è Internet’

Conversazione con *Andrea GHIZZONI*, direttore di WeChat Europa
a cura di *Giorgio CUSCITO*

LIMES Quanto è importante Internet per i cinesi oggi?

GHIZZONI Moltissimo. Rispetto agli occidentali, i cinesi hanno scoperto il Web quando era più maturo. Non si ricordano un mondo senza Internet, né quasi un mondo in cui si navighi senza smartphone. Inevitabilmente, lo usano in tutto quello che fanno durante la giornata. Basta pensare ai milioni di Qr code scansionati al giorno (i codici a barre bidimensionali la cui scannerizzazione digitalizza istantaneamente ogni genere di transazione, incluse quelle delle bancarelle per strada, *n.d.r.*). A ciò si aggiunga che il 97,5% della popolazione cinese accede al Web via smartphone. Nel 2017, 527 milioni di utenti lo hanno utilizzato per eseguire pagamenti. Si tratta di un incremento di quasi il 60% rispetto all'anno precedente¹⁰. Per

10. Cfr. Quarantaduesimo «Rapporto statistico sullo sviluppo della rete Internet in Cina», China Internet Network Information Center, 20/8/2018.

non parlare dei milioni di transazioni al minuto registrate su WeChat. Queste non sono necessariamente realizzate online. Anzi, sono i pagamenti nei punti vendita fisici a crescere maggiormente, attraverso il portafoglio digitale dell'applicazione. Quindi, azioni come pagare il caffè al bar, prendere il taxi o noleggiare una bicicletta si eseguono ormai tramite Internet. Le ore spese sul Web, la componente transazionale e il punto di contatto con il mondo fisico indicano che per i cinesi Internet non è solo uno spazio di azione, ma è parte della quotidianità.

LIMES In questo contesto, che ruolo ha WeChat e che rapporto ha con Pechino?

GHIZZONI WeChat è l'asse portante della comunicazione digitale in Cina, quindi l'interazione con il governo è ragionevolmente stretta. Diversamente da quanto accade in Occidente, nella Repubblica Popolare tendenzialmente non si apre un motore di ricerca per navigare il Web. I cinesi accedono ai servizi digitali soprattutto tramite piattaforme. Molte delle quali si focalizzano su obiettivi specifici. Alibaba o JD per esempio si concentrano sul commercio online. Toutiao è un aggregatore di notizie. Weibo (il Twitter cinese, *n.d.r.*) è un sito di *microblogging*, serve per scambiare idee ed esprimere opinioni. WeChat ha invece il vantaggio di essere la piattaforma più pervasiva e duttile. Include le funzionalità di Internet più altri strumenti. Di fatto, rappresenta il Web come lo disegnerebbe un *millennial*. La prima cosa che fanno i giovani quando accendono lo smartphone è chattare. WeChat è nato come strumento di comunicazione (messaggi di testo, audio e video), ma consente anche di pubblicare contenuti sulla propria bacheca e di cercare nuovi contatti. Inoltre è arricchito al suo interno da «miniprogrammi» e attività di altre piattaforme. Per esempio, permette di eseguire transazioni, ascoltare la musica in streaming integrando l'account Qq Music (equivalente di Spotify, *n.d.r.*), comprare il biglietto dell'autobus o prenotare un ristorante tramite Dianping. Generalmente in Occidente compiamo queste attività tramite applicazioni o siti Web. In Cina, il sistema di WeChat è utile agli operatori economici. Anziché registrarsi su diversi social network per rintracciare i clienti, le aziende si concentrano in un unico punto di ritrovo e attirano l'attenzione più rapidamente. Questo meccanismo conviene anche al consumatore perché semplifica l'utilizzo di Internet. A ciò si aggiunga che un numero elevatissimo di cinesi nel mondo usa WeChat anche se all'estero non può usufruire di tutti i servizi di cui beneficia nella Repubblica Popolare. Questa scelta dipende non solo dal fatto che agevola le comunicazioni con parenti e amici in patria. Per i cinesi, WeChat è una sorta di «campione nazionale» di cui vogliono essere fruitori.

LIMES Perché i social network occidentali non riscuotono molto interesse in Cina?

GHIZZONI Nella Repubblica Popolare, le piattaforme digitali cinesi hanno inizialmente acquisito un vantaggio competitivo perché non è possibile accedere a concorrenti come Facebook, Twitter o Google. Il consumatore della Repubblica Popolare è mediamente più giovane e digitalizzato di quello occidentale. In un ambiente «protetto», le imprese cinesi hanno potuto crescere e adattarsi più rapidamente alle esigenze dell'utente. In questo modo, WeChat è passata dall'essere un'applicazione simile a WhatsApp a offrire una più vasta gamma di funzioni. Per questa

ragione, il consumatore cinese non ha esigenza di cercare le alternative occidentali. Ai suoi occhi rappresentano prodotti più arretrati. Inoltre, c'è differenza tra Ovest ed Est sul tipo di comunicazione più idonea. In Occidente, prevale quella di tipo verticale, che tende a mettere in evidenza la funzionalità che usano più utenti. Gli utenti asiatici esigono un'esperienza diversa, cercano una comunicazione orizzontale. WeChat pone le attività possibili tutte sullo stesso piano, in maniera sequenziale. Anche per questo, all'inizio la piattaforma non è stata compresa all'estero. Eppure oggi anche i social network occidentali stanno sviluppando progressivamente un'impostazione simile. Probabilmente, una volta digerito il cambio di paradigma, europei e statunitensi cercheranno queste funzioni nelle piattaforme già utilizzate e più familiari anziché in WeChat, percepita più lontana culturalmente.

LIMES Le aziende quindi devono essere necessariamente attive sulle piattaforme digitali per fare affari in Cina?

GHIZZONI Decisamente. Le grandi imprese del *made in Italy* sono su WeChat da anni, anche se all'inizio lo consideravano un canale di comunicazione come gli altri. Negli ultimi anni, hanno capito che l'applicazione svolge un ruolo diverso. Ora si chiedono come integrare WeChat nel punto vendita fisico e nelle attività di commercio digitale, come profilare gli utenti cinesi e rispondere alle esigenze del consumatore. Si veda in questo ambito l'apertura della «boutique digitale» o l'utilizzo dell'esperienza aumentata nel negozio. Da qualche tempo, i marchi di fascia media si stanno avvicinando al mondo digitale cinese. In parte, ciò dipende dal fatto che prima era molto complesso ottenere una licenza di account business su WeChat. Ora la procedura è stata in parte snellita e non ha costi particolari. Ciò che ancora rallenta le aziende piccole sono le complessità legate alla strategia di gestione del negozio digitale e il tipo di servizi che si vuole proporre sulla piattaforma.

LIMES Le tensioni in corso tra Usa e Repubblica Popolare sul fronte commerciale e tecnologico possono incidere negativamente sull'andamento dell'economia digitale cinese?


GHIZZONI Non penso. La rapidità con cui la Cina ha sviluppato il suo mondo digitale non ha confronti. Nel campo dell'intelligenza artificiale (Ai), credo che uno dei vantaggi della Cina rispetto agli altri paesi sia che le attività sul Web dei suoi cittadini producono molti più dati e informazioni utili allo sviluppo di algoritmi. Nella Repubblica Popolare, gli utenti di Internet sono 800 milioni, «solo» il 60% della popolazione totale. In secondo luogo, il supporto del governo allo sviluppo tecnologico è molto forte e ciò rende la crescita in questo settore più agevole. A prescindere da quanto accade a livello internazionale, le aziende straniere vogliono fare affari in Cina. A tal fine, hanno bisogno di digitalizzare le proprie attività, così da cogliere le enormi potenzialità del mercato. Basta pensare al fatto che Google ha recentemente investito 550 milioni dollari in JD e potrebbe tornare nella Repubblica Popolare con un nuovo motore di ricerca, d'accordo con Pechino. Inoltre, come ha detto Tim Cook, capo della Apple, è alquanto complicato trovare un altro paese che offra una combinazione di competenze e scala produttiva pari alla Cina. A prescindere dai proclami, le filiere produttive di Repubblica

Popolare e Stati Uniti sono legate. È difficile chiudere le attività in Cina per produrre altrove, magari in cerca di un'altra Foxconn. Apple ha peraltro scelto una strategia diversa rispetto ad altre compagnie tecnologiche occidentali, puntando su una fascia alta di consumatori. È diventata quasi un marchio di lusso. In questo modo, evita di competere con aziende sul piano puramente tecnologico. Altre compagnie occidentali invece rischiano di risentire maggiormente la competizione di concorrenti cinesi come Huawei o Oppo perché si tratta semplicemente di un confronto funzionale tra i rispettivi prodotti.

COME LA RUSSIA PROIETTA LA SUA POTENZA CIBERNETICA

di John BAMBENEK

Dall'Estonia agli Usa, passando per Georgia e Ucraina, i corsari informatici e le agenzie d'intelligence sono le avanguardie di Mosca nel reame cyber. Fra retaggio sovietico, competizione interna, diverse modalità operative e fiaschi recenti. Il caso Skripal.

1.  OCHE POTENZE SONO TEMUTE TANTO quanto la Russia nel campo dell'hackeraggio di Stato. Oggi i corsari informatici del Cremlino rappresentano per abilità e sfacciataggine un vero e proprio unicum nel panorama mondiale della sicurezza informatica, facendo in taluni casi davvero pochissimo per celare le tracce del loro passaggio e tenendo in minima considerazione il rischio di provocare danni collaterali.

Di solito spetta alle unità militari o ai corpi d'intelligence la gestione delle operazioni di attacco cibernetico degli Stati. La gran parte di essi preferisce agire con discrezione e proprio per questo le agenzie di spionaggio sono piuttosto attente a operare nell'ombra. Non è il caso della Federazione Russa, almeno per quanto concerne le operazioni del gruppo di hacker noto come Apt 28 (o Fancy Bear) che si ritiene essere alle dipendenze del Gru, il potente servizio informazioni delle Forze armate federali. Sicuramente più discreto è Apt 29 (o Cozy Bear), che invece dovrebbe essere gestito da agenzie d'intelligence civili con un approccio sicuramente più tradizionale, quali l'Fsb (Federal'naja služba bezopasnosti, erede del sovietico Kgb) o Svr (Služba vnešnej razvedki, il Servizio d'intelligence esterna).

Nel 2016 sia Fancy Bear sia Cozy Bear riuscirono a violare i server del Democratic National Committee statunitense durante le elezioni presidenziali di quell'anno. Allora nessuno dei due gruppi di hacker sembrava essere a conoscenza delle attività dell'altro, anche se il dato più interessante riguarda il modo in cui vennero impiegate le informazioni raccolte. Cozy Bear le mise a disposizione del proprio servizio di analisi: dopo tutto, i partiti politici dei paesi democratici rappresentano pur sempre un'ottima fonte di dati.

Fancy Bear, al contrario, lanciò un'operazione contro il corpo elettorale americano nel tentativo di indirizzare l'esito delle elezioni, con gli operatori del Gru a creare e gestire il profilo Twitter Guccifer_2.0 proprio per inserire la pro-

MAPPA DELLE RIVOLUZIONI COLORATE



pria narrativa nel più vasto dibattito politico americano. Questa informazione è stata trasmessa dall'agenzia russa a WikiLeaks, che ne diede conto in una serie di e-mail rese pubbliche nelle settimane finali della tornata elettorale. Il gruppo di hacker ha quindi lanciato altri attacchi anche in occasione delle elezioni francesi e tedesche.

Di per sé l'attività di raccolta informazioni ai danni di forze politiche straniere non rappresenta alcunché di eccezionale. Il caso invece assume altro rilievo se si considera che Fancy Bear ha scelto di utilizzare i dati raccolti per influire sull'esito delle elezioni della prima potenza mondiale, facendo pochissimo per nascondere il proprio coinvolgimento, forse anche perché sprovvisto della capacità di occultarsi completamente.

Le specificità operative dei due gruppi di hacker aiutano a cogliere un aspetto spesso frainteso della relazione che intercorre fra e all'interno dei servizi di sicurezza russi. In teoria questi vengono considerati come le singole parti del medesimo sistema gerarchico, che opera in maniera uniforme per raggiungere gli scopi decisi dal vertice. La verità, invece, è che nella pratica esiste un certo grado di autonomia unitamente a delle rivalità interne. Individui e gruppi agiscono agli ordini dei loro superiori, ma molto spesso sono liberi di decidere come meglio comportarsi per raggiungere i rispettivi traguardi.

Molti di questi gruppi competono fra loro anche all'interno della stessa agenzia per accaparrarsi influenza, prestigio e risorse. Può anche capitare che finiscano per scontrarsi gli uni contro gli altri, proprio come accadde a due alti ufficiali dell'Fsb che si occupavano di sicurezza informatica e che sono stati arrestati lo scorso anno con l'accusa di tradimento. Si tratta di un semplice esempio del modo in cui priorità concorrenti e rivalità intestine finiscano per produrre conseguenze funeste per la fazione sconfitta.

2. Nel complesso, i ciberattacchi russi tendono a essere rivolti contro i bersagli tradizionali dello spionaggio di Stato: giornalisti, infrastrutture strategiche, parlamenti o corpi legislativi, partiti politici, think tank, Forze armate, agenzie d'intelligence e governi stranieri. Le capacità cibernetiche russe agiscono in primo luogo nelle ex repubbliche sovietiche – spazio che il Cremlino reputa essere la propria sfera d'influenza esterna – ma anche in Europa e in particolare nei paesi Nato, compresi gli Stati Uniti d'America.

In questo senso, soprattutto il Gru e l'Fsb hanno sviluppato e perfezionato le rispettive capacità di condurre operazioni di guerra cibernetica dando vita all'equivalente *cyber* della classica «proiezione di potenza» militare. Tanto che durante ogni conflitto o crisi in cui è stata coinvolta la Federazione Russa nel nuovo millennio gli attacchi informatici hanno fatto abitualmente parte del mix operativo dispiegato contro l'avversario. Trattasi di tecniche che naturalmente sono andate evolvendo nel corso del tempo, passando da rudimentali attacchi comportanti interruzioni di servizio (*denial-of-service*) ad assalti veri e propri alle reti elettriche straniere suscettibili di causare più o meno temporanei blackout.

La crisi fra la Russia e l'Estonia nel 2007 è generalmente considerata il primo esempio di guerra cibernetica al mondo. Fu uno scontro non militare ingenerato dalla decisione estone di trasferire dal centro di Tallinn il memoriale sovietico al Soldato di bronzo e le tombe di guerra, mossa che scatenò le proteste dei filorussi, culminate in un'ondata di attacchi informatici cominciati il 27 aprile.

Attacchi del tipo *denial-of-service* bersagliarono con l'intento di sovraccaricarli i server del governo estone e di società basate nel paese baltico. Alcuni di questi partirono persino da infrastrutture cibernetiche «affittate», impiegate solitamente da criminali informatici. L'Estonia del tempo era un paese già fortemente digitalizzato e ricorreva alla tecnologia anche per le transazioni di routine, un fatto che scaricò le conseguenze degli attacchi sia sulle attività del governo di Tallinn che, più in generale, su quelle della popolazione civile. Le transazioni finanziarie subirono un blocco, molti siti governativi andarono offline e persino il normale ricorso a Internet da parte dei cittadini della repubblica baltica risultò essere pesantemente limitato. Un estone di etnia russa venne condannato per aver preso parte alle incursioni, anche se il Cremlino ha sempre rifiutato qualsiasi forma di cooperazione nelle indagini condotte contro propri connazionali (o almeno da loro considerati tali) accusati di coinvolgimento nelle attività di pirateria informatica.

In maniera analoga, nel 2008, poco prima dell'apertura delle ostilità in Ossezia del Sud, una pioggia di ciberattacchi anticipò il dispiegamento delle truppe russe verso la Georgia. A inizio anno la Russia aveva riconosciuto i governi separatisti dell'Ossezia del Sud e dell'Abkhazia, nonostante le proteste georgiane e dei paesi occidentali. Nei mesi seguenti la crisi crebbe di pari passo alla concentrazione dei reparti militari attorno e dentro la repubblica caucasica, con Tbilisi a rivendicare la propria sovranità sulle province ribelli e Mosca a sostenerne l'indipendenza.

Le operazioni *cyber* scattarono a partire da metà luglio, sia mediante attacchi di tipo *denial-of-service* che tramite manovre di *defacing*, volte cioè ad alterare la *home page* di un sito o le sue sezioni interne. La campagna crebbe in intensità nelle settimane successive, portando più di un analista della comunità di intelligence a lanciare l'allarme sul fatto che diversi siti georgiani erano ormai passati sotto il controllo di entità esterne. In alcuni frangenti, intere porzioni del traffico Internet della Georgia vennero reindirizzate verso la Russia. Frattanto si dipanava una martellante campagna mediatica e di propaganda con cui entrambe le parti reclamavano la propria verità nella crisi.

A inizio agosto, mentre proseguivano i ciberattacchi, il conflitto divenne anche armato. Nel corso dei circa cinque giorni di ostilità militari, il portale del presidente georgiano finì sotto attacco e il suo ritratto ufficiale venne rimpiazzato da un'immagine di Adolf Hitler. Oltre a bersagli governativi furono violati anche i media, con tutte le ripercussioni del caso sul fronte propagandistico mentre sul terreno proseguiva la campagna militare. In Georgia il traffico Internet fu disturbato pesantemente, fatto che rese molto più complicato comunicare con Tbilisi per tutta la durata del conflitto.

Questi attacchi rappresentano la prima chiara prova di una campagna informatica coordinata ad operazioni militari di stampo tradizionale, mentre non è irrealistico pensare che da quel conflitto le capacità *cyber* di Mosca siano avanzate sensibilmente. Difatti, se la varietà e la sofisticazione degli attacchi contro la Georgia attestano la crescita delle abilità russe a soltanto un anno di distanza dalla crisi in Estonia – fatto su cui non possono non aver pesato i continui investimenti operati dal Cremlino nell'arte della guerra cibernetica – la fine delle ostilità nel Caucaso non ha portato con sé alcuna indicazione di una flessione nella quantità di risorse profuse dai russi in *cyberwarfare*.

3. Nel corso degli anni, il Gru è stato accusato di aver violato ripetutamente le reti elettriche dell'Ucraina e di aver causato interruzioni di corrente ai danni del vicino occidentale. Ma nonostante la crisi sullo status della Crimea e il confronto armato nelle province ucraine orientali, queste operazioni non hanno mai sostenuto alcun conflitto militare su larga scala. Piuttosto che ad acquisire un qualche vantaggio tattico su Kiev, gli attacchi furono infatti pensati in primo luogo per dimostrare le capacità russe al resto del mondo. Altro fulgido esempio della sfacciataggine con cui è solito agire il Gru, che rinuncia alla discrezione tipica delle operazioni di intelligence tradizionali per adottare un approccio apertamente muscolare, volto a mettere sotto pressione i rivali della Russia.

In maniera analoga ebbe a svilupparsi l'attacco *ransomware* NotPetya, attribuito anch'esso al Gru e finalizzato a compromettere il software gestionale ucraino MeDoc, utilizzato da quasi ogni società del paese. I creatori del malware impiegavano anche alcuni software trafugati dalla National Security Agency statunitense per favorirne la trasmissione attraverso le reti interne collegate ai computer infetti, rendendo inservibili i dischi rigidi e seminando il caos fra i soggetti colpiti.

È lecito pensare che l'attacco sia stato orchestrato con l'intento precipuo di danneggiare il solo ex socio sovietico, benché successivamente la fragilità della rete Internet ucraina abbia permesso al malware russo di propagarsi anche al resto del mondo, causando danni per miliardi di dollari. In fondo è difficile scorgere altre ragioni che non fossero la volontà di mettere in mostra la propria potenza cibernetica e di punire l'un tempo alleata Ucraina. Ciononostante, visti gli ingenti danni causati alla rete Internet globale, l'attacco ha finito per avere conseguenze indesiderate sulla reputazione della Federazione Russa all'estero.

Durante ciascuno dei sopracitati attacchi, gli hacker russi hanno agito senza mai preoccuparsi dei danni collaterali che avrebbero potuto generare mentre le loro azioni si ripercuotevano puntualmente anche su obiettivi non militari e civili. Se causare interruzioni di corrente in tempo di guerra è considerato un uso improprio del potere militare, produrne in assenza di conflitto significa non avere alcuna considerazione per le vite dei civili o per l'opinione pubblica internazionale.

4. Oggi la Russia può giovare dei frutti dei suoi incessanti investimenti in *cybersecurity* e dei programmi volti a rafforzarne le capacità offensive e difensive.

Già al tempo dell'Unione Sovietica il paese spendeva risorse considerevoli in programmi di crittografia e altre discipline suscettibili di formare un bacino di tecnici altamente qualificato per ogni tipo di operazione. È un fatto che oggi i programmi di sicurezza informatica russi siano reputati fra i migliori al mondo, forse anche perché continuamente messi alla prova da tentativi di violazione.

Sotto quest'ultimo profilo, ad esempio, Mosca ospita ogni anno il forum PHDays ove legioni di hacker competono fra loro in infrazioni simulate di rete elettriche, bancomat e altre infrastrutture strategiche alla base della nostra vita quotidiana. Gare del genere hanno luogo durante qualsiasi raduno di pirati informatici, benché per magnitudine la kermesse moscovita sia senza dubbio ineguagliata al mondo. Insegnando il valore della protezione dei sistemi informatici, PHDays è un ottimo esempio di quali ripercussioni abbiano gli investimenti cibernetici effettuati in Russia, suscettibili naturalmente di soddisfare anche gli interessi del governo.

La quantità di persone con abilità informatiche dentro la Federazione Russa e nelle ex repubbliche sovietiche spiega inoltre come mai svariati cybercriminali provengano proprio da questa parte del mondo. La maggior parte delle principali operazioni illecite orchestrate in Internet è infatti concepita e coordinata dall'interno dei confini federali. Il botnet Zeus e il primo *ransomware* crittografico al mondo, ad esempio, erano gestiti da Evgenij Bogačëv, il pirata informatico russo ricercato da Fbi e Dipartimento di Stato americano.

Un altro caso riguarda Pëtr Levašov, ideatore del botnet Kelihos nonché hacker con alle spalle una carriera quasi ventennale, che è stato arrestato in Spagna nel 2017 prima di essere estradato negli Stati Uniti, dove si è dichiarato colpevole delle accuse di hackeraggio mosse a suo carico. È interessante notare che nel corso degli ultimi dieci anni Levašov abbia lavorato per le campagne elettorali di Russia Unita, il partito di Vladimir Putin. Mentre il cybercrimine e l'hacking di Stato appartengono nominalmente a due sfere distinte, l'esperienza dimostra che fra loro può sussistere anche una forte interazione.

5. Il confine fra agenzie d'intelligence e gruppi criminali è sempre stato poroso, tanto più nel caso della Federazione Russa. La violazione di Yahoo!, ad esempio, è stata gestita da due agenti dell'Fsb che nel 2013 consentirono a semplici criminali informatici di compromettere miliardi di account del portale Web di servizi americani nonostante avessero ricevuto l'ordine di raggiungere obiettivi limitati dai vertici dell'intelligence. Questa operazione è rimasta sconosciuta per anni e c'è voluto ancora più tempo per capire chi l'avesse orchestrata, un tratto in aperto contrasto con le modalità operative del Gru – ben più audaci e facilmente riconoscibili – che inoltre dimostra come gli agenti dell'intelligence russa possano fare affidamento sulle loro controparti nel crimine organizzato per ricevere assistenza operativa.

Spesso, infatti, le entità criminali che operano in Russia mantengono contatti diretti con le agenzie d'intelligence, ricorrendo a pagamenti in denaro per assicurarsi libertà di manovra senza correre il rischio di subire la ritorsione delle autorità oppure scambiando informazioni in cambio di favori. Violando account e computer

di decine di milioni di utenti, un gruppo criminale può entrare in possesso di dati di alto profilo suscettibili di attrarre l'interesse delle agenzie d'intelligence russe.

Queste ultime a volte decidono di reclutare i cibercriminali per impiegarli direttamente al proprio servizio, come attestato dalle lamentele che di tanto in tanto compaiono su alcuni forum governativi. In questo senso il mondo criminale informatico russo fornisce alle agenzie d'intelligence federali un bacino di talenti cui attingere anche in maniera coercitiva e con modalità che sarebbero impensabili per gli standard occidentali. Non è un caso che alcuni fra i pirati informatici più abili al mondo risiedano in Russia o in un'ex repubblica sovietica. Le loro capacità sono tali da consentirgli di realizzare malware molto sofisticati, ricorrendo all'inganno per indurre le vittime a installare software infetti oppure spingerli a compromettersi. La violazione della posta elettronica di John Podesta, quando costui guidava la campagna presidenziale di Hillary Clinton, ad esempio, avvenne tramite l'invio di una falsa mail di reset della password di Google. Un semplice link infetto fornì agli operatori del Gru la chiave per avere libero accesso a tutti i suoi messaggi di posta.

6. Non esistono metodi infallibili per verificare l'identità delle persone che navigano in Rete. Persino in Europa le norme più recenti in materia di privacy hanno se possibile peggiorato la facoltà di giungere a un'autenticazione certa di un dato profilo. Dopo l'entrata in vigore della General Data Protection Regulation non è più possibile ricorrere alla tecnica adottata in precedenza per individuare i falsi profili impiegati dagli hacker russi essendo stata esclusa, proprio in nome della privacy, la possibilità di effettuare controlli indipendenti sulla proprietà di un dato dominio.

Nonostante l'abilità dimostrata in più di una circostanza, nel tempo i gruppi di corsari informatici russi hanno commesso anche diversi errori sia conducendo normali operazioni *cyber* sia quando impegnati in operazioni più complesse. Il che ha causato problemi non indifferenti alla Federazione Russa, come nel caso recente del tentato omicidio di Sergej Skripal nel Regno Unito da parte di agenti del Gru. Non che vi fossero particolari remore morali a colpire un ex ufficiale russo diventato un agente britannico. Il fatto però è che la catena di errori commessa da parte degli aspiranti assassini ha rappresentato un'onta gravissima per la reputazione di un paese reputato maestro in un certo genere di operazioni.


Gli errori e la sfrontatezza degli operatori del Gru hanno avuto un ruolo nella decisione di riassegnare alcuni incarichi all'interno dello stesso servizio informazioni militare, complice probabilmente il desiderio emerso in seno all'agenzia d'intelligence di rivedere parte delle proprie modalità operative. Soltanto il tempo dirà quali saranno le conseguenze pratiche di questi cambiamenti. Quel che è chiaro è che la Russia continuerà a investire nelle proprie capacità offensive *cyber* e a perfezionare la propria abilità di colpire gli avversari con attacchi informatici.

(traduzione di Alberto de Sanctis)

PER UNA GERARCHIA DELLE CIBERPOTENZE

di Matthew CROSTON

Un quintetto di Stati guida le classifiche del potere cibernetico: Usa, Cina, Russia, Israele e Regno Unito. Obiettivi e ipocrisie dell'uso strategico della Rete. L'America resta il bullo più grosso e cattivo nel Web. Chi più fa meno dice: Mosca prenda nota.

1.  QUALUNQUE ANALISI CHE PASSI IN RASSEGNA e compari le potenze cibernetiche più avanzate e attive finisce in fretta per limitarsi ai soliti noti: Stati Uniti, Cina, Russia, Israele e Regno Unito. La ricorrenza di questo quintetto è generalmente dovuta a una combinazione di fattori: da quanto tempo i vari attori hanno iniziato a guardare alla dimensione cibernetica come a un legittimo ambito della potenza e a uno strumento statuale; i sempre maggiori investimenti sia in termini di risorse finanziarie che di personale; la dimostrata assertività nell'utilizzo di questo potere per raggiungere obiettivi strategici.

Almeno dal 2010 gli Stati Uniti si sono impegnati con determinazione a rimanere l'incontestata potenza guida in questo settore. Proprio in quell'anno raggiungeva la piena operatività il Cyber Command, la struttura militare nella quale nel 2009 Washington aveva fuso le disparate unità cibernetiche delle proprie Forze armate. Da quel momento, gli investimenti in questo ambito (non solo sulle capacità difensive, va specificato) hanno cominciato a essere contate nell'ordine dei miliardi di dollari e il personale dedicato è più che quadruplicato. E benché l'America sia riluttante ad ammetterlo pubblicamente, non è una coincidenza che dopo questi sviluppi istituzionali la Cina abbia praticamente copiato il piano a stelle e strisce, promettendo di unificare tutte le proprie capacità e i propri guerrieri cibernetici in una sola struttura e di stanziare massicce risorse finanziarie.

La Russia figura in tutte le analisi non tanto a causa delle dichiarazioni formali in tal senso da parte dei governi cinese e americano, ma in virtù delle crescenti prove dirette e circostanziali della sua volontà di trattare l'arma cibernetica alla stregua di qualunque altro tradizionale strumento bellico o di politica estera. Per rendersene conto, basta osservare quanto fatto in Estonia nel 2007, in Georgia nel 2008, in Ucraina dal 2014 e nelle elezioni presidenziali negli Stati Uniti nel 2016. L'ironia di tanto attivismo è che l'attore che in questo campo sembra più determi-

nato a mantenere l'attuale livello di segretezza sui propri sviluppi e investimenti cibernetici non è stato altrettanto in grado di cancellare le proprie tracce quando ha effettivamente usato tali strumenti nell'arena mondiale.

Questo paradosso – tale solo all'apparenza – ci porta di fronte a uno dei maggiori tratti che distinguono le cinque potenze elencate in partenza. Quattro di esse sono relativamente trasparenti sull'importanza del potere cibernetico, ma sono altrettanto intente a farne uso in segreto. La Russia, invece, non è per nulla trasparente, ma ha sempre finito per esporle in pubblico quando le ha impiegate a sostegno dei propri interessi.

Per molti versi, Israele può essere considerato la potenza più silenziosa del quintetto: in pochi tendono a riconoscere non solo l'aggressività di Gerusalemme nell'erigere la propria strategia difensiva attorno a capacità cibernetiche offensive, ma anche il fatto che allo Stato ebraico pertenga il 10% delle vendite mondiali di computer e tecnologie di sicurezza delle reti. Infine, il Regno Unito figura nella lista in gran parte a causa di due considerazioni. Primo, gli intensi e stretti legami politici con gli Stati Uniti e con Israele. Secondo, le enormi somme investite nell'incrementare i propri strumenti cibernetici nello scorso decennio, fino a essere senza dubbio indicato come lo specialista europeo del settore.

2. Se non c'è molto dibattito su chi faccia parte del quintetto di vertice, si può invece discutere su come ordinarne i membri in base alla sofisticatezza dei rispettivi arsenali cibernetici. Inevitabilmente, il livello di segretezza che li circonda costringe in parte questo esercizio al livello delle congetture. Tuttavia, alla base di una possibile classifica c'è un importante elemento che viene spesso sottovalutato in Occidente: l'elettrico clima politico che si genera attorno all'uso del potere cibernetico.

Gli Stati Uniti mantengono una linea molto delicata e forse leggermente ipocrita: dichiarano l'intenzione di conservare il dominio in questo campo su tutti gli altri paesi, investono cospicuamente nelle armi offensive potenzialmente più letali, eppure non vogliono che gli altri paesi si preoccupino di tale preminenza. Per esempio, la principale divisione cibernetica del panorama delle spie a stelle e strisce, la National Security Agency (Nsa), possiede un gigantesco quartier generale a Fort Meade che non è solo armato, ma dispone della propria forza di polizia indipendente. Il numero degli impiegati al suo interno equivale a una piccola città. Questa burocrazia si accresce sempre più col passare del tempo, tanto che l'Nsa ha recentemente unito le proprie forze con quelle del già menzionato Comando cibernetico. Le rivelazioni dello scandalo Snowden hanno anche dimostrato che l'agenzia non disdegnerebbe che Internet fosse trasformato in un enorme campo di battaglia, con i soli Stati Uniti a godere di un autentico dominio su questo nuovo territorio. La stessa organizzazione ha quantomeno dato il via ad alcuni programmi volti a impiegare i metadati intercettati per scopi spionistici «non intrusivi» nei confronti dei propri connazionali.

Il punto è che la postura cibernetica americana, sia in termini strategici che operativi, è presumibilmente la più aggressiva al mondo. Ma le critiche in tal senso

sono mute se paragonate a quelle che si levano contro due bersagli ricorrenti come la Cina e la Russia. Certo, questi due attori non se ne stanno con le mani in mano e sono molto attivi nell'utilizzo del potere cibernetico per avanzare i propri interessi e avvantaggiarsi in diverse partite. Mosca si è concentrata molto di più sui risultati politici e militari delle proprie missioni cibernetiche; mentre Pechino si è rivelata l'indiscusso campione dello spionaggio economico, del furto di proprietà intellettuale e dell'ingegneria inversa per acquisire la tecnologia necessaria a competere sui mercati globali. Ma qui non si tratta di scagionare l'operato dei due Stati né di ridimensionare la portata delle loro operazioni. È invece affascinante notare quante poche critiche vengano riservate agli Stati Uniti mentre questi ultimi si assicurano la più avanzata e paralizzante forza cibernetica del pianeta. La narrazione americana funziona più o meno come segue: «Ci stiamo dotando delle armi necessarie a disincentivare comportamenti cibernetici criminali da parte di altre nazioni». Davanti a questa argomentazione potrebbe non essere corretto dimostrarsi del tutto scettici. Tuttavia, è innegabile come la potenza statunitense stia anche spingendo paesi come Cina, Russia e Iran a cercare di compensare le capacità di Washington. L'ostinata ricerca da parte dell'America di tutto ciò che la conservi come il dominante poliziotto cibernetico del mondo potrebbe dunque stare approfondendo una competizione globale per sviluppare armi sempre più raffinate.

Quando si osservano il ruolino di marcia e le capacità degli Stati Uniti in questo settore, c'è davvero da meravigliarsi che non ci si preoccupi di più degli obiettivi manifesti di Washington. Consideriamo tre aspetti.

Primo. Lontano dai riflettori, l'America ha aggressivamente cercato di dare alle proprie armi cibernetiche una più spiccata componente offensiva. Stuxnet, il virus lanciato contro le centrifughe nucleari iraniane, è stato solo il primo, piccolo tassello di questo mosaico ed è estremamente probabile che gli siano succeduti *malwares* molto più affilati.

Secondo. Non importa quanti altri paesi investano nello sviluppo delle proprie forze cibernetiche. La loro somma comunque impallidisce se paragonata a quanto gli americani spendono ogni anno in questo ambito. È dunque corretto affermare che gli Stati Uniti non stanno davvero competendo con altri Stati in termini di pianificazione strategica di lungo periodo: proprio come nell'iniziale fase di sviluppo dell'arsenale nucleare, Washington non vuole che ci sia alcun dubbio su chi sia in grado di intraprendere operazioni cibernetiche unilateralmente nel momento ritenuto necessario e senza temere di pagare un gran prezzo.

Terzo. La sfacciataggine con cui gli Stati Uniti hanno condotto operazioni di spionaggio cibernetico, campagne di «influenza maligna» e intercettazioni in giro per il mondo – a volte pure contro paesi tecnicamente alleati o «amici» come Germania e Messico – è finito sulle prime pagine di tutti i media e ha causato una discreta dose di imbarazzo pubblico. Tutto ciò non ha alcun impatto sulle future operazioni, ma fa venire al resto del pianeta più di un dubbio quando Washington punta il dito contro altri Stati per aver orchestrato missioni simili contro il territorio o soggetti americani. Cina, Russia, Corea del Nord, Iran, pure Israele

hanno subito accuse del genere negli ultimi anni. Nelle conferenze globali a cui non partecipano relatori statunitensi la lamentela più comune è diretta contro questo smaccato doppiopesismo.

La Cina sta molto attenta a rivolgere tali critiche a Washington, probabilmente perché non vuole attirare su di sé ancor più attenzione di quanta già non ne ricevano le sue attività economiche in ambito cibernetico. Non è invece il caso della Russia, che alza sempre la voce e si schiera in prima fila per accusare gli americani di dire una cosa e fare l'esatto contrario. Per i russi, gli Stati Uniti sono di gran lunga la più aggressiva ciberpotenza del pianeta e rifiutano seccamente la narrazione secondo cui nessuno dovrebbe preoccuparsi delle politiche cibernetiche americane perché sono generalmente volte al bene del mondo. Va sottolineato come né Mosca né Washington si stiano impegnando a contenere le proprie capacità o a dare il la a una convenzione internazionale volta a sviluppare norme per il ciber-spazio che limitino equamente il ricorso a questo strumento. Al contrario, i due attori combattono per il modo in cui i rispettivi stili cibernetici vengono caratterizzati: gli americani non vogliono essere criticati e pretendono il beneficio del dubbio; i russi vorrebbero che il mondo riconoscesse che essi fanno esattamente ciò che fanno gli Stati Uniti nell'ombra.

3. Se dunque si rimuove dall'equazione il modo in cui i vari attori si atteggiavano pubblicamente, è sufficiente ammettere che le potenze del quintetto sono attive nel ciberspazio per scopi buoni e meno buoni, ma sempre per il proprio esclusivo interesse.

In quest'ottica, gli Stati Uniti sono l'hacker superpotente: hanno tutto il denaro, il talento, la motivazione per dominare questo territorio e la posizione in cui si trovano non li spaventa affatto. La Cina è l'hacker economico, principalmente intenta ad aumentare la propria posizione relativa nel sistema economico globale. Anche se ciò non vuol dire che il suo raggio di azione si fermi all'ambito pecuniario. Per esempio, benché lo neghi ufficialmente, è opinione corrente negli Stati Uniti che la Repubblica Popolare abbia hackerato le Forze armate a stelle e strisce sottraendo i piani dell'F-35. Un furto che, stando ai militari americani, ha direttamente portato allo sviluppo del caccia cinese J-31. Come spesso accade in questo mondo, non esistono pistole fumanti, ma le prove circostanziali suggeriscono fortemente questa conclusione.

La Russia, invece, è l'hacker politico spavaldo che, come del resto in altri campi, cerca di vedersi riconosciuta la propria ciberpotenza. In quest'ottica, quando Mosca nega il coinvolgimento nei sabotaggi di Estonia, Georgia e Ucraina non lo fa per reclamare la propria innocenza, ma per rifiutare ogni tipo di critica: quando è impegnato in un conflitto – prosegue il ragionamento – uno Stato ha il diritto di impiegare qualunque strumento abbia a propria disposizione. Secondo questa interpretazione, la natura delle relazioni internazionali è sempre stata così e tale deve rimanere. Dunque, per i russi, la potenza cibernetica non è qualcosa a sé stante, ma semplicemente un'estensione di ciò che già esiste.

Per converso, il Regno Unito tende a essere qualificato come l'hacker guardingo, molto qualificato nel raccogliere importanti volumi di informazioni ma non particolarmente portato ad agire di conseguenza. La caratterizzazione va presa con le pinze: vista la già menzionata vicinanza agli Stati Uniti e a Israele, il fatto che i britannici non impieghino attivamente le informazioni che rastrellano non significa che quelle informazioni non vengano impiegate da altri.

Il che ci porta appunto a Israele, l'hacker geopolitico, eminentemente preoccupato dall'uso delle capacità cibernetiche per proteggersi dal livello di ostilità e aggressività proprio della regione in cui sorge. La trasformazione della Rete in un campo di battaglia ha aggiunto nuove tensioni e requisiti difensivi per lo Stato ebraico, soprattutto nella sua sfida con l'Iran. Stuxnet è un perfetto esempio di come Gerusalemme impieghi strumenti cibernetici in modo collaborativo: benché il virus sia stato realizzato dall'Nsa americana, sono stati gli israeliani ad assicurarsi che esso raggiungesse la destinazione prefissata e distruggesse le centrifughe della centrale nucleare di Natanz.

La Corea del Nord merita una negativa menzione d'onore, in qualità di hacker aggressivo e disperato, essendosi per anni appoggiata a capacità cibernetiche tutto sommato avanzate per riempire le proprie vuote casse – essere bollati come Stato canaglia ha un costo. Si stima che il 10-15% delle sue riserve di valuta estera provengano direttamente da attività cibernetiche illegali. Il furto da 81 milioni di dollari alla banca centrale del Bangladesh, l'intrusione nella Sony, l'infame attacco *ransomware* WannaCry (ironicamente frutto di un'arma rubata all'Nsa) è emblematico di quale sia l'attuale scopo dei talenti cibernetici coltivati a P'yŏngyang. È anche il motivo per cui i nordcoreani non figurano nella lista delle ciberpotenze mondiali: fintanto che il loro status internazionale rimarrà inalterato, è probabile che i loro sforzi nella Rete resteranno a un livello criminale, senza sfociare negli intrighi politici.

4. Sin qui ci siamo concentrati sulle sottigliezze e sfumature da adottare per avere un quadro più chiaro del quintetto delle ciberpotenze. Per concludere occorre però gettare uno sguardo sulle ricerche in corso che stanno provando a sviluppare idee più chiare su che cosa ci sia al di là di questi cinque attori. La İstanbul Teknik Üniversitesi (İtu) ha recentemente pubblicato una delle analisi sin qui più complete in tal senso, volta a valutare e categorizzare sistematicamente l'intero ciber spazio adottando le lenti del potere politico¹. La Itu ha impiegato una matrice a 11 entrate per stabilire tre attributi del possesso e della proiezione del potere cibernetico: difesa, attacco e dipendenza. I paesi sono stati classificati in base alle seguenti variabili e valutazioni:

- bilancio cibernetico allocato alle Forze armate;
- spesa militare complessiva;

1. B. ÇELİKTAŞ, N. ÜNLÜ, «Cyber Security Power Ranking by Country and Its Importance on World Politics», *The Journal of Academic Social Science Studies*, n. 67, primavera 2018, pp. 469-488.

- classifiche di sviluppo tecnologico;
- Global Cybersecurity Index;
- rapporto McAfee sulla difesa cibernetica;
- tasso popolare di impiego di Internet;
- classifiche di sviluppo delle industrie di software;
- traffico di attacchi cibernetici.

Impiegando tanti dati provenienti da ambiti così diversi del potenziale cibernetico di uno Stato, gli studiosi sono stati in grado di produrre una categorizzazione delle ciberpotenze che finalmente va oltre le tipiche valutazioni concentrate sul quintetto discusso finora. Nonché oltre l'abusata distinzione fra queste cinque potenze e gli attori cibernetici «canaglia» sia statali che non – un calderone di casi di studio in cui solitamente finiscono sia uno Stato come la Corea del Nord sia gruppi come lo Stato Islamico.

Così concepita, la potenza cibernetica si suddivide in quattro livelli.

- Livello 1: Usa, Cina, Russia.
- Livello 2: Francia, Regno Unito, Israele.
- Livello 3: India, Corea del Sud, Corea del Nord, Germania, Turchia.
- Livello 4: Brasile, Canada, Italia, Giappone, Iran.


L'aspetto forse più impressionante è che lo studio si spinge persino a classificare individualmente i paesi a seconda dei vari gruppi di dati interrogati. Ciò ci permette di considerare la profondità, l'adattamento, il cambiamento e la diversità dei vari attori, laddove in precedenza l'analisi era piuttosto statica e monotona. Ricerche come queste stabiliscono inoltre che il potere cibernetico sul palcoscenico mondiale è destinato a diventare sempre più contestato e la lotta per accaparrarselo sarà sempre più convulsa. Il che, onestamente, non può essere ritenuto uno sviluppo positivo. Il quintetto classico delle potenze si è fin qui meritato l'attenzione dell'opinione pubblica, ma questo scrutinio deve essere urgentemente espanso, poiché senza dubbio un numero maggiore di concorrenti farà presto il proprio ingresso in grande stile in quest'arena. Anche se un dato sembra essere immutato: nel futuro prossimo, il bullo più grosso e più cattivo in ambito cibernetico resterà l'America.

(traduzione di Federico Petroni)

LA CIBERFIONDA DI DAVID

di Luca MAINOLDI

Producendo il virus Stuxnet, nel 2010 Israele si dimostrò superpotenza cibernetica. Da allora ha saputo mantenere tale status. Attraverso lo sforzo congiunto di Forze armate, intelligence, politica e start-up. All'origine di tutto, lo shock provocato dalla guerra del Kippur.

1.  ENERGIA È UNO DEI PRINCIPALI pilastri delle economie; di alcune ne è il sistema cardiovascolare¹, ha affermato nel giugno di quest'anno l'ex capo dell'Unità 8.200, il generale Ehud Schneorson, lasciando intendere che Israele avrebbe la capacità di colpire con proprie armi ciberetiche le infrastrutture energetiche iraniane. Quella del generale a riposo sembra quasi una rivendicazione tardiva dell'attacco al sistema di controllo delle centrifughe per l'arricchimento dell'uranio di Natanz, condotto tra il 2005 e il 2010 con il sofisticato virus informatico Stuxnet.

Stuxnet non è solo la prima arma cibernetica impiegata nella storia a fini strategici, ma anche il frutto di un'estesa collaborazione tra almeno due superpotenze di prim'ordine, Stati Uniti e Israele, e tra agenzie di Stati diversi. Il virus è stato prodotto, sperimentato e inoculato nelle centrifughe del complesso di Natanz, in un'operazione complessa effettuata da Cia e Nsa da parte americana, e da Mossad e Unità 8200 da parte israeliana. Secondo alcuni ufficiali dell'Aviazione americana, all'iniziativa avrebbe partecipato pure il Regno Unito, per cui «Washington e Londra hanno fornito tecnologia, risorse e fondi mentre Gerusalemme ha offerto gestione del programma, continuità nell'operazione, strutture per test e addestramento, nonché il quadro legale per lanciare l'attacco»².

Lo sforzo realizzato dai due (o tre) paesi è frutto di un accordo politico negoziato da George W. Bush e proseguito da Barack Obama, al fine di rallentare in modo surrettizio il programma iraniano di arricchimento dell'uranio e costringere Teheran al tavolo negoziale.

1. Cfr. Y.J. BOB, «Ex-“Israeli NSA” Chief: Target Iran, Hezbollah Energy Infrastructure First», *Jerusalem Post*, 18/6/18.

2. Cfr. D.A. FULGHUM, «Searching for Ways to Trace Cyber Attackers», *Aviation Week*, 20/5/11.

Secondo un esperto americano con una lunga esperienza nel campo dei programmi militari segreti, lo Stato ebraico avrebbe avuto la capacità di sviluppare un'arma cibernetica del genere anche da solo: «Israele può pescare dal suo complesso militare e industriale i talenti necessari per creare una squadra che si concentri su di un problema fino a risolverlo. Talent che hanno la disciplina per studiare un problema, costituire strutture per l'addestramento, sperimentare le possibili soluzioni finché non trovano quella giusta e finché non realizzano l'attacco»³. Il coinvolgimento di Washington nell'ambito dell'Operazione Olympic Games (questo il suo nome in codice da parte statunitense) aveva un significato geopolitico ancor prima che tecnico: dimostrare agli israeliani che la superpotenza era attivamente impegnata nell'ostacolare i progetti nucleari militari iraniani, scongiurando così un attacco aereo contro i siti atomici della Repubblica Islamica da parte di Gerusalemme.

A sua volta Israele ha potuto dimostrare di disporre di capacità e risorse necessarie per partecipare alla pari con le due potenze anglosassoni nel primo vasto sabotaggio di una struttura fisica per mezzo di un'arma cibernetica. Oltre a Stuxnet sono stati scoperti almeno altri due virus informatici creati per colpire il programma nucleare iraniano: Duqu e Flame. Due programmi spia che hanno permesso di raccogliere le informazioni utili a preparare l'assalto. Ma mentre il primo sembra essere stato realizzato dallo stesso team che ha messo a punto Stuxnet, il secondo invece pare il risultato di un gruppo di lavoro diverso, anche se condivide alcuni dei codici di Stuxnet. Testimonianza di uno sforzo vasto, diversificato e prolungato nel tempo.

2. L'ecosistema cibernetico dello Stato ebraico è frutto di molteplici fattori. Ma il principale è lo shock che Israele, le sue Forze armate e l'intera popolazione hanno subito con l'attacco a sorpresa da parte araba nella guerra dello Yom Kippur (1973). Tzahal e la comunità d'intelligence israeliana furono colti alla sprovvista non solo dall'assalto delle truppe egiziane lungo le rive del Canale di Suez e di quelle siriane sulle alture del Golan, ma anche dalle performance dei missili anti-carro e soprattutto antiaerei forniti dai sovietici ai due eserciti arabi.

L'elaborazione d'urgenza di tattiche specifiche e la fornitura di contromisure elettroniche da parte americana permisero all'Aeronautica israeliana di dominare le difese aeree avversarie, a prezzo di perdite sostenute soprattutto nella fase iniziale del conflitto⁴. A seguito della guerra del Kippur Israele decise di incrementare lo sviluppo della propria industria elettronica militare e civile. Non è forse un caso che nell'anno successivo alla guerra fu fondata la prima filiale israeliana dell'Intel americana. Sempre sull'onda del medesimo shock, qualche anno dopo due professori dell'Università ebraica di Gerusalemme, Felix Dothan e Shaul Yatziv, lanciarono il programma Talpiot per selezionare e formare l'élite di scienziati e tecnici destinati a servire nella Mafat, l'unità di sviluppo tecnologico di Tzahal, considera-

3. *Ibidem*.

4. Solo la Marina riuscì a prevalere contro i missili antinave avversari grazie alle contromisure elettroniche messe a punto per tempo con il concorso italiano.

ta una vera e propria Darpa israeliana. Dopo nove anni di servizio nel Talpiot (la ferma minima richiesta), numerosi membri di questa unità, che unisce alla formazione militare corsi avanzati di matematica e fisica, furono assunti da aziende ad alta tecnologia o fondarono proprie start-up. Tra queste ve ne sono diverse che tuttora operano nel campo della sicurezza cibernetica.

Se Talpiot rappresenta il «meglio del meglio» dell'offerta formativa a disposizione dei giovani israeliani da parte di Tzahal, la maggioranza dei ciberguerrieri israeliani è addestrata da due unità specializzate dell'Aman, l'intelligence militare. L'Unità 8.200, spesso descritta come il contraltare israeliano dell'Nsa americana, è incaricata di intercettare le comunicazioni di soggetti nemici, neutrali e amici, nonché di svolgere attività offensive ad ampio raggio nel campo informatico. L'Unità 8.200 dispone di un reparto di ricerca, soprannominato «The Farm», incaricato di trovare mezzi e modalità sempre nuovi per aggirare le protezioni crittografiche dei sistemi di comunicazione militari e civili, comprese applicazioni come WhatsApp e Telegram. The Farm lavora anche a beneficio dell'ancor più segreta Unità 8.100 che si occupa di penetrare i sistemi di comunicazione e di stoccaggio dei dati di singole organizzazioni e individui.

Dopo aver a lungo dibattuto se formare un unico comando cibernetico responsabile delle azioni difensive e offensive, recentemente i militari hanno deciso di desistere. L'Unità 8200 continuerà a occuparsi delle operazioni offensive di spionaggio e sabotaggio, mentre la Direzione C4I (comando, controllo, comunicazioni, informatica e intelligence) rimane responsabile della difesa delle reti militari.

La svolta tecnologica impressa dall'intelligence militare ha coinvolto anche le due agenzie civili: il servizio di sicurezza interna, lo Shin Bet, e il Mossad, dedicato allo spionaggio e alle operazioni speciali. Il primo ha sviluppato rilevanti capacità nel campo della sorveglianza elettronica e cibernetica, da solo o in collaborazione con lo spionaggio militare.

Lo Shin Bet è passato addirittura per ben tre rivoluzioni digitali, la prima alla fine degli anni Novanta per far fronte all'ondata di attentati suicidi commessi da Hamās. Ora siamo alla terza rivoluzione con la fusione della branca responsabile della Sigint (lo spionaggio elettronico) con quella incaricata delle operazioni difensive e offensive nel ciberspazio. Nel corso degli anni lo Shin Bet si è specializzato nell'intelligence dei social media (Socmint) per prevenire attentati da parte di formazioni terroristiche e di singoli individui. Al momento il 25% del personale dello Shin Bet è impiegato nella branca Sigint/Cyber.

La protezione delle reti civili è condivisa tra l'Autorità cibernetica del direttorato nazionale e lo Shin Bet. La prima, che dispone di un team di pronta risposta con sede a Be'er Sheva, è responsabile della protezione dei due terzi delle infrastrutture vitali del paese, comprese quelle energetiche ed elettriche; il secondo del restante terzo, comprese le infrastrutture delle telecomunicazioni.

A sua volta il Mossad dispone di un segretissimo reparto hacker che, analogamente a quello dell'Unità 8100, prende di mira le comunicazioni e i dati di singole persone o organizzazioni. Il Mossad intrattiene relazioni con alcuni hacker esterni

cui appalta molteplici operazioni, così da mantenere un grado di separazione tra la propria organizzazione e i bersagli colpiti. Di recente il Mossad ha creato un fondo d'investimento sulla falsariga di In-Q-Tel, il braccio finanziario della Cia nella Silicon Valley. Annunciato nel giugno 2017, Libertad Ventures consente al Mossad di relazionarsi con le dinamiche start-up israeliane del Silicon Wadi. Situazione quasi paradossale perché molte delle società nel campo informatico e della sicurezza cibernetica sono state create da giovani che hanno servito nelle due unità di spionaggio elettronico dell'Aman, una volta tornati alla vita civile.

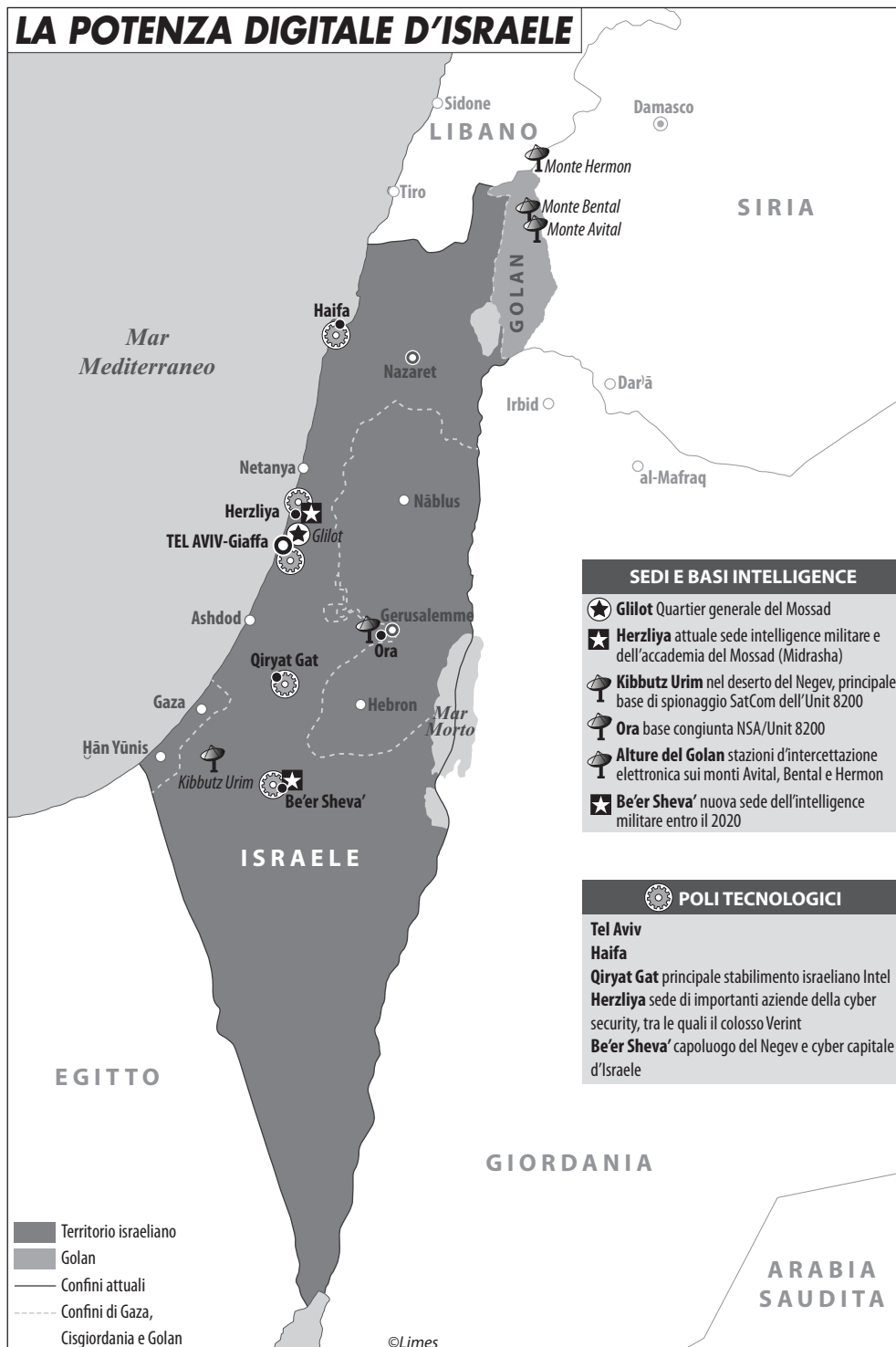
Inizialmente gli ex membri dell'Unità 8200 potevano addirittura commercializzare le invenzioni messe a punto durante il servizio militare. Dagli anni Novanta lo Stato rimane proprietario dei brevetti sviluppati dall'intelligence elettronica, ma gli specialisti che lasciano le due unità sono agevolati nella creazione di società di sicurezza informatica. Naturalmente questi mantengono un legame con i reparti in cui hanno servito durante la leva. Anzi, chi di loro aveva assunto un'identità fittizia con la quale interagire nella Darknet, la può conservare una volta tornato alla vita civile.

Creare e conservare un'identità fittizia nella Darknet non è semplice. Occorrono tempo e sforzi non banali per essere accettati nei forum di discussione della zona scura del Web, dove hacker si scambiano informazioni su falle informatiche e su possibili bersagli, dove trafficanti di droga ed armi incontrano i loro clienti e così via. Conservando la propria fittizia identità digitale un ex combattente cibernetico mantiene una rete di contatti da sfruttare nel suo impiego da civile. Questo garantisce alle società israeliane un netto vantaggio sulla concorrenza. Come capita a Kela Israeli Intelligence e a Clearsky, specializzate nella sorveglianza della Darknet, quell'ampia porzione della Rete, non indicizzata dai comuni motori di ricerca, dove gli utenti navigano seguendo specifici protocolli di sicurezza.

3. Determinante il ruolo di Binyamin Netanyahu nella crescita del settore cibernetico israeliano. Nel 2010 Bibi incaricò il professore Isaac Ben-Israel, capo del Centro interdisciplinare di ricerca cibernetica Blavatnik (Icrc) dell'Università di Tel Aviv, di elaborare un piano per rispondere alle minacce che si potevano materializzare nei successivi cinque anni. Il professore rispose che in ambito informatico tale lasso di tempo equivale a tre o quattro generazioni tecnologiche, per cui è impossibile predire quali sfide potranno materializzarsi. Tuttavia Ben-Israel suggerì di costituire «un ecosistema tecnologico che sappia reagire quando queste minacce imprevedibili si materializzeranno». E il professor Eviatar Matania fu incaricato di creare il necessario layout sotto la direzione del primo ministro⁵.

Bibi colse l'occasione per unire gli sforzi cibernetici all'obiettivo di trasformare una delle zone più depresse del paese, il deserto del Negev, in un centro d'eccellenza tecnologica. Il 3 settembre 2013 alla cerimonia di inaugurazione del

5. La prossima sfida tecnologica che Israele vuole cogliere è quella dell'intelligenza artificiale. Netanyahu ha incaricato ancora una volta Ben-Israel e Matania di elaborare un piano nazionale per collocare lo Stato ebraico tra le prime cinque potenze mondiali nel campo dell'AI.



Parco di tecnologia avanzata dell'Università Ben-Gurion di Be'er Sheva' Netanyahu annunciò la decisione del suo governo di trasformare la principale città del Negev in un centro nazionale e internazionale per la cibernetica e la cibernsicurezza, in cui convogliare una parte cospicua degli investimenti esteri nel settore high tech israeliano.

A tal fine le Forze armate nel Negev hanno varato un vasto piano per spostare dall'area costiera al deserto circa 30 mila militari, appartenenti all'élite di Tzahal, oltre a squadroni di aerei da combattimento e di supporto; e la quasi totalità dei reparti dell'intelligence militare, compresa l'Unità 8.200 e il Centro per i sistemi informatici e di computer delle Forze armate. Il trasferimento avviato nel 2015 si protrarrà ancora per alcuni anni. Finché l'85% della forza lavoro dell'Aman sarà trasferita nei pressi di Be'er Sheva', dove numerose aziende americane, tedesche, cinesi, giapponesi hanno già creato centri di ricerca presso il parco tecnologico della locale università.

Sotto la guida dell'Autorità cibernetica nazionale⁶, un ente controllato dall'ufficio del primo ministro, si è sviluppato un complesso ecosistema cibernetico formato da enti statali (esercito e intelligence), da centri universitari di ricerca, e da società piccole e grandi che forniscono servizi specializzati (l'intercettazione dei cellulari) o a spettro più ampio (sicurezza informatica integrata a forme di sicurezza fisica).

A loro volta i grandi gruppi della Difesa, come la Israel Aerospace Industries (Iai) o la Elbit, hanno costituito apposite divisioni di sicurezza cibernetica. Il tutto per raggiungere l'obiettivo fissato da Netanyahu di collocare Israele tra le prime cinque ciberpotenze mondiali. Un successo raggiunto almeno a livello commerciale, perché tra il 2013 e il 2017 le aziende israeliane hanno conquistato il 7% del mercato mondiale della cibernsicurezza, occupando il secondo posto delle vendite globali dietro a quelle statunitensi, che con il 69% si collocano al primo posto. Il Regno Unito è terzo con il 6%. Peraltro a questo si aggiunge un altro dato: il 20% degli investimenti mondiali nella cibernsicurezza va ad aziende israeliane.

Il settore cibernetico è a sua volta parte della più vasta offerta di prodotti e servizi per la sicurezza da parte di società israeliane legate ai tre principali servizi d'intelligence statali. L'offerta del complesso industriale-militare-securitario è ampia: dalla consulenza per filiali di multinazionali in zone a rischio di controspionaggio industriale alla protezione di strutture fisiche, come stazioni e aeroporti, e di strutture virtuali come le reti informatiche private o statali; dalla fornitura e gestione di sistemi d'intercettazione telefonica e informatica alla produzione di virus informatici da inoculare negli smartphone per trasformarli in apparecchi spia. Fino all'addestramento di reparti militari e di intelligence di Stati esteri. Accanto alle start-up fondate da ex coscritti dell'intelligence vi sono società costituite e dirette da ex dirigenti militari e dei servizi di sicurezza, che mettono a disposizione la propria rete di contatti tessuta in tutto il mondo.

6. Alla fine del 2017 l'Autorità cibernetica nazionale è stata aggregata all'Autorità di cibernsicurezza nazionale (Ncsa), andando a costituire il ciberdirettorato nazionale.

Una delle ultime nate nell'ambito della ciberdifesa è Toka, tra i cui fondatori vi è Ehud Barak, il generale più decorato d'Israele ed ex primo ministro e ministro della Difesa. Toka, annunciata pubblicamente a luglio, ha subito raccolto 12,5 milioni di dollari. Oltre a Barak, tra i suoi fondatori figura il generale Yaron Rosen, già responsabile per lo staff cibernetico di Tzahal. Secondo Rosen la nuova azienda ambisce «ad aiutare gli Stati esteri a sviluppare capacità strategiche, un approccio operativo e un ecosistema di prodotti software concepiti su misura per loro», precisando che i laboratori cibernetici di Toka svilupperanno prodotti adatti ai propri clienti se sul mercato ancora non esistono. Grazie agli investitori e al suo management Toka intende diventare un'interfaccia tra Stati sprovvisti di capacità cibernetiche difensive (e offensive) e le aziende israeliane attive nel settore, riservando per sé il campo emergente della sicurezza dell'Internet degli oggetti (IoT).

Il governo israeliano sostiene pienamente gli sforzi commerciali delle aziende del settore a fini economici ma anche geopolitici. L'Agenzia per lo sviluppo internazionale del ministero degli Esteri (Mashav) fornisce programmi di formazione e di consulenza per la cibersicurezza a paesi in via di sviluppo. I legami che si creano in questo campo tra attori stranieri pubblici e privati ed entità commerciali israeliane rafforzano i rapporti internazionali dello Stato ebraico. La scoperta che i servizi segreti degli Emirati Arabi Uniti e dell'Arabia Saudita impiegano un malware di produzione israeliana per spiare gli smartphone è probabilmente solo la punta dell'iceberg di una relazione molto più estesa e profonda.

Per vendere i loro prodotti in paesi che non mantengono relazioni diplomatiche con lo Stato ebraico, le aziende israeliane hanno creato apposite società in Europa occidentale ed orientale, specie in Svizzera, in Ucraina e in Bielorussia. In questo modo Israele aumenta le capacità di raccolta informativa e di azione della propria intelligence statale. Inoltre, almeno in teoria, mantenere buone relazioni in un settore così delicato permette alle agenzie d'intelligence israeliane di creare delle «porte di servizio» attraverso le quali introdursi nelle reti di altri paesi, spiando le operazioni dei servizi di sicurezza locali o sfruttando server e computer stranieri come base per lanciare operazioni spionistiche e di sabotaggio contro i propri avversari.

Israele ha avviato una vera e propria offensiva diplomatica per rafforzare in tutto il mondo i legami in ambito di cibersicurezza. Specie attraverso Cybertech, la più significativa conferenza non americana di cibertecnologie, che dal 2014 si tiene a Tel Aviv e che è stata replicata a Singapore, in Europa e nelle Americhe. Quest'anno Roma ha ospitato per la terza volta consecutiva l'edizione europea, a testimonianza dei forti legami stabiliti da enti pubblici e privati italiani e israeliani nell'ambito della sicurezza informatica.

Con gli Stati Uniti, Israele ha di recente creato un forum bilaterale sul tema. Le aziende americane hanno acquistato diverse start-up (tra queste Waze) ed effettuato imponenti investimenti in Israele dove Intel, Microsoft, Apple e Google hanno importanti centri di ricerche. Inoltre, le società americane di *venture capital* si ag-
giungono alle omologhe e dinamiche società israeliane nel finanziare le nuove

imprese. A loro volta aziende dello Stato ebraico hanno investito nella Silicon Valley, in Texas e a Boston, sviluppando rapporti con enti privati e pubblici, federali e dei singoli Stati.

In Asia, è Singapore l'hub strategico per le imprese israeliane che intendono conquistare i mercati orientali, specie la Corea del Sud, l'India, le Filippine e la Thailandia. Nella città-Stato la Iai ha creato un centro per la cibersicurezza e i due paesi intrattengono da decenni stretti legami nel campo della difesa e dell'intelligence, esteso all'ambito cibernetico.

Altro Stato chiave è il Giappone, dopo l'intesa siglata nel 2014 tra Netanyahu e Abe Shinzō che prevede la formazione in Israele di esperti giapponesi in sicurezza informatica e la consulenza da parte dello Stato ebraico per la protezione virtuale delle prossime Olimpiadi di Tōkyō 2020. I due governi hanno pure creato un forum di dialogo sul tema.

In Europa, in vista del Brexit il Regno Unito sta rafforzando le proprie relazioni industriali e di sicurezza con alcuni Stati chiave, Israele compreso, con il quale il governo britannico intende collaborare allo sviluppo di tecnologie per l'industria 4.0, comprendenti l'intelligenza artificiale e la cibersicurezza. Inoltre Londra, insieme a New York, è un'importante piazza finanziaria per le start-up israeliane in cerca di fondi. In Francia alcune società israeliane sono fornitrici dei servizi governativi, nonostante le diffidenze legate allo scontro tra aziende dei due paesi sui mercati africani. Mentre durante la sua recente visita in Israele Angela Merkel ha ribadito il desiderio di rafforzare i legami con lo Stato ebraico in campo tecnologico e cibernetico.

Infine la Cina costituisce una sfida e un'opportunità. Se pure nel 2017 la Repubblica Popolare contava un terzo degli investimenti nel settore high tech israeliano, secondo lo Shin Bet le maggiori minacce nel campo cibernetico per lo Stato ebraico proverrebbero proprio da Russia e Cina, non da Iran o Ḥamās. Hacker cinesi avrebbero rubato alcuni segreti dei sistemi antimissili Iron Dome e Arrow 3. Così in Israele si è aperto un dibattito sugli investimenti della Repubblica Popolare nel settore high tech e nelle infrastrutture nazionali, per timore che lo spionaggio di Pechino li usi per sottrarre segreti industriali e militari. Persino i sistemi intelligenti di regolazione del traffico installati da aziende cinesi in alcuni importanti snodi stradali dello Stato ebraico possono veicolare all'intelligence dell'Impero del Centro informazioni su movimenti militari o sull'innalzamento del livello d'allarme delle truppe di Tzahal. Insomma Israele dovrà presto decidere da che parte schierarsi, quando l'alleato americano intensificherà ulteriormente il confronto a tutto campo con Pechino.

li·M·es
in più

SE SI AMMALA LA PELLE DEL PIANETA

di Pietro TINO

I processi di inaridimento del suolo, particolarmente accentuati nella fascia intertropicale, mettono a rischio la sopravvivenza di ampie porzioni d'umanità. Le origini del fenomeno. La crisi del magnese. Serve un ripensamento del modello agricolo e urbano.



A CIVILTÀ HA LE SUE FONDAMENTA nel sottile strato superficiale di suolo che ricopre parte del pianeta» e «la salute dei popoli che ci vivono non può essere separata dalla salute del suolo stesso»¹. Non vi è alcuna forma di enfasi nella considerazione di Lester Russel Brown, uno dei più attenti indagatori delle trasformazioni ambientali e autorevole rappresentante della cultura scientifica della sostenibilità, fondatore del Worldwatch Institute e successivamente dell'Earth Policy Institute. Benché estranea o poco familiare alla cultura dominante, nella quale la presenza della materialità della natura nella vita degli uomini è assente o del tutto marginale, la considerazione di Lester Brown mette in luce un elemento decisivo nella storia delle società. Anche prescindendo dalle molteplici funzioni ecologiche, che ne fanno uno dei principali nodi degli equilibri ambientali, è infatti dal suolo fertile, dal suo uso produttivo che proviene il cibo quotidiano per il sostentamento dell'umanità. Risorsa fondativa della vita, il suolo è al contempo, dati i tempi estremamente lunghi (geologici) della sua formazione e rigenerazione, una risorsa non rinnovabile. Dalla sua conservazione, dalla preservazione della sua fertilità e della sua salute – già gravate dalla crescente domanda alimentare globale che per il solo effetto della crescita demografica, senza cioè considerare il verticale aumento del consumo medio pro capite, si è all'incirca settuplicata nel corso degli ultimi due secoli² – dipende quindi il futuro dell'umanità.

1. L.R. BROWN, *Piano B 4.0. Mobilitarsi per salvare la civiltà*, Milano 2010, Ed. Ambiente, pp. 72, 74.

2. Da circa 1 miliardo all'inizio del XIX secolo (1804), la popolazione della Terra è aumentata a 2 miliardi nel 1927 e a circa 7,3 miliardi nel 2015 (M. LIVI BACCI, *Il pianeta stretto*, Bologna 2015, il Mulino, pp. 18-19, 27, 29).

Un fenomeno globale, tra passato e presente

Risorsa naturale limitata, non rinnovabile e insostituibile, la «pelle viva del pianeta» con i suoi pochi centimetri di spessore è attraversata da profondi e preoccupanti processi di degrado delle sue capacità produttive, del quale la desertificazione costituisce il punto finale. L'erosione dei suoli e la riduzione della loro fertilità non è però un fenomeno nuovo. Antico quanto il mondo, esso ha subito una prima accelerazione attorno al 2000 a.C., con la diffusione dell'agricoltura dalle valli fluviali ai ripidi declivi e ai terreni boscosi della Cina, dell'Asia meridionale, del Medio Oriente e delle regioni attorno al Mediterraneo. Si è poi ulteriormente allargato ed accentuato a partire dalla fine del XV secolo, con la scoperta del nuovo mondo e l'espansione coloniale europea. Si è infine dilatato, assumendo dimensioni inedite per ampiezza e intensità, nel corso del Novecento e soprattutto dalla sua seconda metà, con lo sviluppo dell'agricoltura commerciale nelle terre marginali dei tropici, l'adozione generalizzata delle lavorazioni meccaniche con mezzi pesanti, l'affermazione diffusa di indirizzi produttivi a carattere intensivo e monoculturale, alimentati e sostenuti dal massiccio impiego di concimi chimici e prodotti fitosanitari³.

Di questa crescente accelerazione dell'erosione dei suoli, il verticale aumento della perdita di humus (le sostanze organiche del terreno, decomposte o in via di decomposizione, all'origine della sua fertilità) costituisce un indice di rara eloquenza: da circa 25 milioni di tonnellate l'anno prima della rivoluzione industriale, la dissipazione di sostanza organica si è elevata a ben 300 milioni l'anno nei secoli XIX e XX, fino a raggiungere 760 milioni di tonnellate l'anno nella seconda metà del Novecento⁴.

Secondo le Nazioni Unite, oltre il 25% delle terre coltivate del pianeta – e ben il 70% delle terre aride coltivabili – è colpito dalla desertificazione, «mettendo a repentaglio il sostentamento di più di un miliardo di persone, in particolare dei contadini e dei pastori di circa cento paesi»⁵. Ogni anno circa 10-12 milioni di ettari di terra vengono investiti da processi di degrado della loro fertilità⁶. Il fenomeno è particolarmente grave in Africa, Asia, Sudamerica, Caraibi, ma interessa anche gli Stati Uniti, l'Australia e l'Europa, in particolare quella mediterranea.

3. Per le fasi, qui richiamate, che hanno scandito la storia dell'erosione dei suoli, cfr. J.R. McNEILL, *Qualcosa di nuovo sotto il sole. Storia dell'ambiente nel XX secolo*, Torino 2006, Einaudi, pp. 42-62; S. MOSLEY, *Storia globale dell'ambiente*, Bologna 2013, il Mulino, pp. 87-127; per l'erosione dei suoli delle regioni attorno al Mediterraneo in età antica si vedano le considerazioni di C. PONTING, *Storia verde del mondo*, Torino 1992, Società Editrice Internazionale, pp. 88-91, nonché le indicazioni di L. THOMMEN, *L'ambiente nel mondo antico*, Bologna 2014, il Mulino, pp. 42-43 e *passim*.

4. D. MEADOWS, D. MEADOWS, J. RANDERS, *I nuovi limiti dello sviluppo. La salute del pianeta nel terzo millennio*, Milano 2006, Mondadori, p. 87. Un quadro globale dei processi di erosione del suolo, ma con riferimento allo stato del fenomeno all'inizio degli anni Quaranta del secolo scorso, è fornito da G.V. JACKS, R.O. WHYTE, *Quando la terra muore. Il problema mondiale dell'erosione del suolo*, Milano 1947, Mondadori.

5. L.R. BROWN, *Un mondo al bivio. Come prevenire il collasso ambientale ed economico*, Milano 2011, Ed. Ambiente, p. 70.

6. B. CROCE, S. ANGIOLINI, *La Terra che vogliamo. Il futuro delle campagne italiane*, Milano 2013, Ed. Ambiente, p. 18.

Nell'Africa subsahariana, a causa della crisi di fertilità del suolo – determinata in larga misura dall'accresciuto sfruttamento originato dalla crescita demografica e attuato mediante una drastica limitazione della pratica rigeneratrice del maggese – circa 265 milioni di persone sono colpite da carenze alimentari⁷. La sola Nigeria, la nazione più popolosa del continente africano con oltre 190 milioni di abitanti, perde ogni anno, a causa della desertificazione, oltre 350 mila ettari di pascoli e di terreni agricoli coltivabili⁸. Gran parte delle migrazioni che muovono da quelle regioni verso l'Europa o altre destinazioni sono prodotte dalla crisi di fertilità dei suoli coltivabili e dei pascoli.

L'effetto dei crescenti processi di desertificazione non si concreta tuttavia solo nelle migrazioni, negli spostamenti in direzioni diverse di intere comunità e popolazioni. Tra espansione demografica – con il conseguente aumento della domanda di cibo – desertificazione e altre forme di degrado o di sottrazione definitiva dei terreni alla produzione alimentare, la terra fertile è diventata una risorsa scarsa, quindi fortemente appetibile. Da qui il *land grabbing*, l'impressionante quanto inquietante corsa di Stati e multinazionali all'accaparramento, generalmente nei paesi poveri o in via di sviluppo, di terre arabili. Fenomeno, anche questo, non nuovo, che ha accompagnato episodicamente la storia del colonialismo tra Ottocento e inizi Novecento; ma che nell'ultimo quindicennio ha assunto peculiarità e dimensioni del tutto inedite e assolutamente straordinarie, divenendo esso stesso causa di espulsioni di un gran numero di contadini e di intere comunità, nonché – stante l'adozione di un uso agricolo a carattere intensivo e monoculturale – di immani processi di degrado ambientale e spesso di morte definitiva degli stessi terreni. Secondo alcune stime, soltanto tra il 2006 e il 2011 sono stati acquisiti da imprese private e governi stranieri ben 200 milioni di ettari di terra coltivabile, soprattutto in Africa ma anche in America Latina e in diversi paesi asiatici⁹. Per meglio rendersi conto delle dimensioni del fenomeno può essere utile osservare che si tratta di una superficie quasi doppia rispetto alla somma della superficie territoriale della Francia e della Spagna.

Ma quali sono le cause della desertificazione? È opportuno notare che il termine desertificazione non rimanda solo all'allargamento del perimetro del deserto, cioè di una realtà ecologica preesistente che si espande e inghiotte aree contermini prima coltivate. Fenomeno, anche questo reale e preoccupante, che si manifesta un po' ovunque, dal Sahara al deserto del Gobi in Cina, generando altre imponenti teorie di rifugiati o migranti ambientali¹⁰. Esso sta piuttosto a indicare – ed è

7. R. BUNCH, «La crisi della fertilità del suolo in Africa e la carestia imminente», in *State of the World 2011. Nutrire il Pianeta*, Worldwatch Institute, Milano 2011, Ed. Ambiente, p. 163.

8. L.R. BROWN, *9 miliardi di posti a tavola. La nuova geopolitica della scarsità di cibo*, Milano 2012, Ed. Ambiente, p. 85.

9. S. SASSEN, *Espulsioni. Brutalità e complessità nell'economia globale*, Bologna 2015, il Mulino, pp. 91-128. Sul *land grabbing* cfr. anche S. LIBERTI, *Land grabbing. Come il mercato delle terre crea il nuovo colonialismo*, Roma 2011, minimum fax; P. DE CASTRO, *Corsa alla terra. Cibo e agricoltura nell'era della nuova scarsità*, Roma 2012, Donzelli, pp. 105-151; A. ASCHIERI, M. LELIÈVRE, *La fin des terres. Comment mangerons-nous demain?*, Paris 2012, Éd. Scrineo, pp. 13-28.

10. L.R. BROWN, *Un mondo al bivio*, cit., pp. 112-113.

questo che qui si intende – la «degradazione progressiva» delle caratteristiche dei suoli arabili nei loro diversi aspetti – meccanici, fisici, chimici e biologici – quale esito delle interazioni tra fattori naturali e attività umane. Come recita la definizione adottata dalla Convenzione dell'Onu per la lotta alla desertificazione (United Nations Convention to Combat Desertification, Unccd), firmata a Parigi il 14 ottobre 1994, «il termine desertificazione designa il degrado delle terre nelle zone aride, semi-aride e sub-umide secche provocato da diversi fattori, tra i quali le variazioni climatiche e le attività antropiche»¹¹.

Fattori come il clima e le attività umane, favoriti o meno nei loro effetti negativi dalle peculiarità ambientali dei singoli contesti territoriali (profilo orografico, disponibilità idrica, natura dei suoli e del relativo substrato), sono dunque all'origine del progressivo degrado della fertilità dei suoli. Le condizioni climatiche non sono del resto indipendenti dalla vita degli uomini, dato che tra le cause del loro mutamento vi è proprio l'attività umana. Quest'ultima è dunque l'origine principale dei processi di erosione dei suoli. In molte zone della fascia intertropicale della Terra, l'area di maggior concentrazione dei fenomeni di desertificazione, accanto all'immane deforestazione (che ha radicalmente modificato i quadri ambientali preesistenti¹²) e all'uso agricolo a carattere intensivo e monoculturale (che ha accompagnato e accompagna la *land grabbing*), una delle cause principali dell'inaridimento risiede nel crescente sfruttamento della terra determinato dalla sostenuta crescita demografica che si è dispiegata a partire dalla seconda metà del Novecento. La coltivazione pressoché ininterrotta e il conseguente abbandono della pratica di lasciare ciclicamente i terreni a riposo per consentirne la rigenerazione hanno prodotto gravi conseguenze su terre generalmente poco profonde e bisognose del continuo apporto di sostanza organica.

«Il dramma attuale di molte regioni tropicali», scrivevano agli inizi di questo millennio Claude e Lydia Bourguignon, «è il tragico accorciamento del maggese. In Asia, sulle montagne del Laos o del Vietnam, in America centrale, sulle montagne del Guatemala o del Messico, in Africa, sul monte Camerun o in Ruanda, la durata del maggese scende sotto i dieci anni e la natura non ha il tempo di ricreare una fertilità. L'erosione assume proporzioni inquietanti che si traducono nella desertificazione inesorabile di queste regioni e spinge i piccoli agricoltori ad abbandonare i campi per ammassarsi nelle *bidonvilles*»¹³.

11. *United Nations Convention to Combat Desertification*, Paris, 14/10/1994, art. 1, goo.gl/kCR2Nn (ultimo accesso, per tutte le fonti elettroniche, gennaio 2018). Cfr. anche T. CECCARELLI, F. GIORDANO, A. LUISE, L. PERINI, L. SALVATI, *La vulnerabilità alla desertificazione in Italia: raccolta, analisi, confronto e verifica delle procedure cartografiche di mappatura e degli indicatori a scala nazionale e locale*, Apat – Agenzia per la protezione dell'ambiente e per i servizi tecnici, Roma 2006, p. 11.

12. Dal 1950 agli inizi del XXI secolo sono stati disboscati «più di 5 milioni di chilometri quadrati di foresta tropicale», un'estensione pari a circa nove volte la superficie della Francia e a oltre sedici quella dell'Italia, in larga parte per produrre derrate agricole da esportare, destinate all'alimentazione o (come nel caso della canna da zucchero e della soia) per estrarre biocarburanti, ma anche per ricavare legname da costruzione e pasta di legno per il mercato di consumo dei paesi sviluppati. Cfr. S. MOSLEY, *op. cit.*, pp. 49-85 (citazione a p. 59).

13. C. e L. BOURGUIGNON, *Il suolo: un patrimonio da salvare*, Bra (Cn) 2004, Slow Food Editore, p. 167.

In Africa, con un indice di ruralità ancora intorno al 60% della popolazione complessiva, l'incremento demografico – oltre il 364% tra il 1950 e il 2010, contro una media mondiale di circa il 174%¹⁴ — si è tradotto, specie nelle regioni centrali, in una drastica riduzione della «quantità di terra che ogni famiglia può coltivare»¹⁵. Ciò ha determinato una duplice conseguenza: la riduzione, nelle singole conduzioni, delle superfici a pascolo, con la conseguente diminuzione del bestiame allevato e della disponibilità di letame per la reintegrazione della fertilità dei suoli; una forte intensificazione dello sfruttamento dei suoli stessi attraverso il prolungamento del periodo di coltivazione e la drastica limitazione del maggese. «Per gran parte degli agricoltori africani», riferisce Roland Bunch, «i periodi di maggese sono passati dai 15 anni degli anni Settanta ai circa 10 negli anni Ottanta e ad appena 5 negli anni Novanta. Oggi, la maggior parte di loro può tenere a maggese i terreni 2 anni al massimo e molti non possono permettersi nemmeno questo»¹⁶. In un contesto pedologico già fragile, contraddistinto da «una debole fertilità intrinseca», l'esito – assecondato dal cambiamento climatico che altera i regimi delle precipitazioni e per nulla mitigato dall'impiego esiguo di concimi minerali – è la rapida riduzione, fino al totale esaurimento, della fertilità e capacità produttiva dei suoli¹⁷.

Italia e dintorni

In misura diversa, dipendente appunto dall'interazione tra peculiarità locali dei fattori naturali e attività antropiche, tutta l'Europa meridionale è percorsa da larghi e avanzati processi di degrado. Oltre al Portogallo, tutti i territori europei che chiudono il Mediterraneo, dalla Spagna all'Italia alla Grecia, ne sono variamente interessati. Vastissime regioni denotano ormai un tenore di sostanza organica, il costituente più importante e l'indicatore chiave dello stato di salute dei suoli, inferiore all'1%¹⁸, chiara espressione di un incipiente stato di desertificazione e inaridimento. Il Sud del Portogallo, tutta la vasta sezione centro-meridionale della Spagna, l'Italia e gran parte della Grecia sono le regioni maggiormente investite dal fenomeno. In Spagna, uno dei paesi europei più colpiti, secondo le stime del Ministerio de Agricultura, Alimentación y Medio Ambiente il processo di degrado delle terre coltivabili – espresso da un indice di rischio medio, alto e molto alto – interessa circa il 37% dei suoli nazionali e si concentra per grandissima parte nella regione centrale e mediterranea¹⁹.

14. E. VANHAUTE, *Introduzione alla World History*, Bologna 2015, il Mulino, pp. 50, 114.

15. R. BUNCH, *op. cit.*, p. 161.

16. *Ibidem*.

17. *Gestion de la fertilité des sols pour la sécurité alimentaire en Afrique subsaharienne*, Fao – Organisation des Nations Unies pour l'alimentation et l'agriculture, Rome 2003, pp. 1-12 (p. 1 per la citazione).

18. B. CROCE, S. ANGIOLINI, *op. cit.*, pp. 19-20. Ben il 45% circa del totale dei suoli europei, costituito in grande prevalenza dalle regioni che si affacciano sul Mediterraneo, è contrassegnato da tenori di sostanza organica «bassi o molto bassi» (*ivi*, pp. 21-22).

19. *Impactos del cambio climático en los procesos de desertificación en España*, Gobierno de España – Min. de Agricultura, Alimentación y Medio Ambiente, Madrid 2016, p. 2, www.mapama.gob.es

In Italia il fenomeno non è meno rilevante e lo stato di salute dei suoi suoli è spesso assai precario. Oltre il 21% del territorio «è ritenuto a rischio desertificazione»²⁰ e i dati disponibili per l'ultimo decennio del secolo scorso «evidenzia[no] – secondo l'Ispra – una tendenza evolutiva [dei suoli] verso condizioni di maggiore vulnerabilità ambientale»²¹. Sempre secondo l'Ispra, «circa l'80% dei suoli italiani ha un tenore di CO [carbonio organico] minore del 2%», cioè «basso» (tra l'1 e il 2%) e «molto basso» (inferiore all'1%)²². Considerato che per garantire l'efficienza del terreno agricolo il livello di carbonio organico, pari a circa il 60% della sostanza organica presente nei suoli stessi, dovrebbe essere almeno pari al 2%, «la situazione – riferisce l'Ispra – appare preoccupante»²³.

Già agli inizi degli anni Duemila (ma la denuncia potrebbe essere retrodatata di qualche decennio) l'Apat, l'Agenzia per la protezione dell'ambiente poi sostituita dall'Ispra, sintetizzava così lo stato di salute dei suoli dell'Italia: «Buona parte dei suoli italiani presenta preoccupanti problemi di degradazione a causa di una gestione territoriale poco attenta nell'adottare i principali criteri di conservazione del suolo. Il processo di modernizzazione dell'agricoltura, pur fondamentale dal punto di vista produttivo, e una pianificazione urbanistica generalmente poco propensa alla valutazione delle problematiche dei suoli, hanno condotto, in diversi casi, all'innescio di fenomeni degradativi anche molto spinti»²⁴.

Le regioni meridionali e insulari sono quelle dove i processi di desertificazione si manifestano con intensità e ampiezza di gran lunga maggiori che nel resto del territorio nazionale, benché condizioni di preoccupante degrado connotino anche i suoli di vaste aree dell'Italia centro-settentrionale. In Abruzzo, Campania e Calabria, così come nelle Marche, in Emilia-Romagna, Umbria e Sardegna, tra il 30 e il 50% dei suoli è a rischio desertificazione. Tale soglia sale al 55% in Basilicata, al 57% in Puglia e al 58% in Molise, per toccare il livello massimo in Sicilia, dove ben

20. *Un quinto dell'Italia a rischio desertificazione*, 17/6/2017, goo.gl/dbCPS2; E.A.C. COSTANTINI, F. URBANO, G. BONATI, P. NINO, A. FAIS (a cura di), *Atlante nazionale delle aree a rischio desertificazione*, Inea – Istituto Nazionale di Economia Agraria, Roma 2007, pp. VI, 97.

21. *Annuario dei dati ambientali 2016*, Ispra – Istituto superiore per la protezione e la ricerca ambientale, Roma 2016, cap. 10, p. 28, www.isprambiente.gov.it. Cfr. anche L. SALVATI, T. CECCARELLI, L. PERINI, *Sostenibilità dell'agricoltura, fattori di pressione e sensibilità alla desertificazione in Italia. Un indicatore multidimensionale a livello comunale*, Cra – Consiglio per la ricerca e la sperimentazione in agricoltura, Ufficio centrale di ecologia agraria, Roma 2006, pp. 43 ss. e L. SALVATI, «Paesaggio e desertificazione: la geografia del rischio in Italia», 26/2/2013, *Protectaweb*, www.protectaweb.it, che forniscono un quadro analitico dell'incremento dell'indice di rischio o di sensibilità alla desertificazione del territorio italiano dal 1960 al 2010.

22. *Annuario dei dati ambientali 2014-2015*, Ispra, Roma 2015, cap. 10, p. 11, www.isprambiente.gov.it

23. *Ibidem*.

24. *Annuario dei dati ambientali 2005-2006*, Apat – Agenzia per la protezione dell'ambiente e per i servizi tecnici, Roma 2006, p. 765. «I due terzi dei suoli del nostro Paese – riferiva la stessa Agenzia qualche anno prima – presentano preoccupanti problemi di degradazione. (...) È evidente che la modernizzazione dell'agricoltura degli ultimi 30 anni, se nell'immediato ha portato a un aumento produttivo, nel lungo termine ha prodotto, in alcuni casi, tangibili fenomeni di degradazione del suolo e quindi dell'ambiente. D'altro canto anche la pianificazione "urbanistica" del territorio (aree industriali e urbane con le relative infrastrutture) raramente, in particolar modo in passato, ha tenuto conto dell'impatto ambientale prodotto, soprattutto per quanto concerne il suolo» (Ib., *Annuario dei dati ambientali. Edizione 2002*, Roma 2002, p. 350).

il 70% circa della superficie è contrassegnato da «un grado medio-alto di sensibilità alla desertificazione»²⁵. È, del resto, nelle regioni meridionali che si concentra circa il 40% dei suoli italiani investiti da conclamati processi di degradazione, aggiungendo un nuovo elemento ai tradizionali fattori esplicativi del divario Nord-Sud.

Tra le attività umane che hanno contribuito a determinare un così vasto deterioramento dell'equilibrio fisico-chimico-biologico dei suoli italiani e in particolare di quelli meridionali, un ruolo di rilievo, comune a tutta l'Europa mediterranea, lo hanno avuto (e continuano ad averlo) le radicali trasformazioni che hanno contrassegnato la pratica agricola a partire dalla metà del Novecento: la separazione tra allevamento e agricoltura, con il conseguente crollo della concimazione letamica; la diffusione di indirizzi produttivi monocolturali e in particolare di quelli cerealicoli; la generale diffusione delle lavorazioni meccaniche, esercitate con mezzi pesanti anche su terreni declivi, privati delle tradizionali sistemazioni ed esposti così ai processi di ruscellamento delle acque; l'uso ingente della chimica di sintesi (fertilizzanti, pesticidi, insetticidi)²⁶. Queste e altre pratiche tipiche dell'agricoltura industriale (alle quali se ne potrebbero aggiungere altre di diverso segno come gli incendi²⁷), intensificate nei loro effetti depauperativi dalla tendenziale estremizzazione climatica degli ultimi decenni, sono all'origine dei processi di desertificazione del territorio italiano. Essi reclamano – nel Mezzogiorno forse più che altrove, stante la sua maggiore vulnerabilità pedologica e l'accentuata aridità climatica – misure politiche ed economiche capaci di arrestarne e invertirne il decorso, attraverso forme di gestione dei suoli capaci di garantirne la vitalità produttiva e la relativa conservazione.

Ma il problema va ben oltre l'ambito regionale o nazionale. Esso assume dimensioni globali, per la sua ampiezza e per gli effetti sulla geografia insediativa della popolazione. Come tale va affrontato, mediante politiche che riflettano le peculiarità socio-economico-ambientali dei paesi interessati, ma nella ferma e generale consapevolezza che dalla salute della «pelle viva» della Terra dipende la salute e il futuro delle comunità che vi abitano e dell'intera umanità.

25. *Annuario dei dati ambientali 2016*, cit., cap. 10, pp. 29-30. Nelle altre regioni – Toscana, Friuli-Venezia Giulia, Lazio, Lombardia, Veneto e Piemonte – la quota dei suoli a rischio desertificazione oscilla tra il 10 e il 25% e scende a livelli molto contenuti – tra il 2 e il 6% – in Liguria, Valle d'Aosta e Trentino-Alto Adige (*ibidem*).

26. P. TINO, *Le radici della vita. Storia della fertilità della terra nel Mezzogiorno (secoli XIX-XX)*, Soveria Mannelli 2015, Rubbettino, pp. 75 ss.

27. Con andamento altalenante, dal 1970 al 2014 il territorio italiano è stato teatro di 391.777 incendi boschivi (mediamente oltre 8.700 l'anno), che hanno incenerito una superficie (boschiva e non) di 4.680.638 ettari, pari al 15,5% della superficie territoriale e al 23% della superficie agricola e forestale nazionale (*Annuario dei dati ambientali 2016*, cit., cap. 8, pp. 104-105).

AAA SUPEREROI ITALICI CERCANSI

di *Sebastiano CONTRARI*

Nei decenni il fumetto nazionale ha conosciuto varie stagioni e alterne fortune, ma non ha mai prodotto campioni positivi assimilabili a quelli americani. Complesso post-bellico? Scetticismo neorealista? Le tirature calano, ma il potere evocativo resta.

1. ANNI FA AVEVAMO EVIDENZIATO COME la scuola fumettistica italiana (una tradizione di tutto rispetto a livello mondiale, subito dopo quelle giapponese, americana e franco-belga) si caratterizzasse per grandi autori, ma nessun grande personaggio tipicamente italiano¹. Difatti, a partire dal secondo dopoguerra quasi nessun eroe concepito da autori nostrani, da *Tex* a *Dylan Dog*, era italiano per natali o ambientazione. In questo anche il fumetto sembrava specchio della difficoltà della nostra fiction (letteraria in primis, ma anche cinematografica e televisiva) a creare eroi nazionali. Anche nel fumetto, il nostro immaginario collettivo non disponeva di alcun equivalente di Guglielmo Tell, d'Artagnan o Robin Hood. Una lacuna non da poco, considerato che «da quando esiste l'uomo, i miti e gli eroi sono il fondamento di ogni educazione morale»².

Se mancavano gli eroi, *a fortiori* scarseggiavano anche i supereroi. Sotto le Alpi non era mai nato un Capitan Italia, se non in forma parodistica, e i personaggi che indossavano la calzamaglia sono stati più criminali che vigilanti alla Batman.

Negli ultimi anni, tuttavia, qualcosa si è mosso: in parallelo con un ritorno di interesse letterario e del piccolo-grande schermo, nell'ultimo decennio anche nel mondo delle nuvolette tricolori si è registrata una diffusione di personaggi italiani, e da ultimo supereroi, anche se negativi.

Facciamo un passo indietro. Nei primi del Novecento il nostro fumetto ha avuto anche dei personaggi italiani, come il Signor Bonaventura³, ma questa ten-

1. S. CONTRARI, «Il fumetto italiano: grandi maestri, piccoli eroi», *Limes*, «L'impero dei pasdaran», n. 5/2006, pp. 271-288.

2. Così si esprime il Don Chisciotte di Berardi e Milazzo in «Ken Parker – La terra degli eroi», *Ken Parker magazine*, 24-25/1995, gennaio-febbraio. Cfr. S. REGAZZONI, *Sfortunato il paese che non ha eroi*, Firenze 2012, Ponte alle Grazie.

3. Personaggio creato da Toffolo nel 1917 e seguito da Sor Pampurio nel 1929. Oltre a personaggi genericamente italiani come questo, nelle riviste per bambini del primo Novecento vi erano perso-

denza era stata amplificata (coartatamente) durante il fascismo. Tra l'autunno del 1938 e la primavera del 1939, le direttive del Minculpop avevano infatti portato a un'italianizzazione forzata dei personaggi d'Oltreoceano⁴ e poi alla creazione di personaggi nazionali, alcuni dei quali smaccatamente fascisti⁵, anche nell'aspetto fisico⁶ e nel carattere, oltre che nel formato narrativo⁷.

Appariranno così anche le avventure – anch'esse non aliene da intenti propagandistici⁸ – dei primi super forzuti tricolori. In particolare *Dick Fulmine* (di Carlo Cossio e Vincenzo Baggioli, che uscendo nel marzo 1938 precederà di qualche mese il primo numero di *Superman, sic!*) e il suo epigono *Furio Almirante* (creato nel 1940 da Cossio e Gian Luigi Bonelli).

Nel secondo dopoguerra, venuti meno i vincoli autarchici imposti dal fascismo, i fumettisti di casa nostra si riaprono al mondo a stelle e strisce, arrivando per contrappasso a nascondersi sotto nomi anglosassoni⁹ e danno vita a personaggi e avventure ambientate nel grande continente¹⁰ e pubblicate su testate seriali.

Figlio emblematico di questa tendenza è *Tex Willer*, creato nel 1947 da Gianluigi Bonelli e Aurelio Galeppini (dapprima a striscia e poi a partire dal 1958 in albi di 96 pagine a volumetto, che diventerà il formato bonelliano per antonomasia¹¹), che rappresenta tuttora il fumetto principale della casa editrice (fondata dal figlio Sergio), e forse in assoluto quello più venduto in Italia. Come altri personag-

naggi di carattere più astratto (come Quadratino, creato da Rubino nel 1908), assieme alla traduzione dei fumetti americani. Da notare l'importanza di tali riviste anche sul piano editoriale: il *Corriere dei Piccoli* si affermò come il più diffuso settimanale di fumetti europeo. Cfr. M. STEFANELLI, «L'italiano nelle nuvole», *la Repubblica* 29/10/2017.

4. The Phantom diventa così L'Uomo Mascherato, Tim Tyler e Spud Slavins vengono ribattezzati Cino e Franco e Brick Bradford cambia nome in Guido Ventura. Infine, Superman viene presentato come Ciclon o l'Uomo Fenomeno (venendo attribuito a Vincenzo e Zenobio Biaggioli) e Tarzan come Sigfrido.

5. Si pensi alle propagandistiche storie del pilota Romano (di Caesar), o alle storie ambientate nella guerra d'Abissinia (come *I tre di Macallé*, che sostituirono Flash Gordon sull'*Avventuroso*). Non mancarono tuttavia lavori non schierati e di buona fattura come gli adattamenti di classici letterari o dei cicli salgariani e opere di fantascienza, come *Saturno contro la terra*.

6. Furio Almirante cambiò la propria fisionomia (in particolare addolcendo la mascella, ritenuta evidentemente poco italica), salvo poi recuperarla nel 1947.

7. Le direttive imposero pure la sostituzione dell'uso dei fumetti con le didascalie, nonché quella delle parole straniere.

8. Vi è chi ha contrapposto il modello superomistico americano, tendenzialmente individualista e ispirato a un'etica universale, con le finalità diverse connesse alla costruzione (e all'esaltazione) dell'uomo nuovo fascista, funzionale alla gloria della nazione e pertanto inscindibile dalla dimensione collettiva. Cfr. G. SPONZILLI, *Il mito del supereroe: Dal fumetto al cinema italiano contemporaneo*, Roma 2017, Ed. Mediterranee.

9. Rinaldo Dami diventa così Roy D'Ami, Leo Cimpellin Alex Loyd, Cesare Solini Phil Anderson, Antonio Canale Tony Chan e Franco Donatelli Frank Well, mentre Gianluigi Bonelli si firma alternativamente come B. O'Nelly, Big John e J.B. O'Selly.

10. Dopo *Gim Toro* (personaggio nato nel 1946 con caratteristiche tutto sommato di transizione, essendo italo-americano), abbiamo l'*Asso di Picche* (sotto il cui costume si nasconde il giornalista Gary Peters), Plutos (il cui vero nome è Bill Donovan), *Tanks l'uomo d'acciaio* (alias Jack Hilton) e *Misterix* (dietro cui si nasconde John Smith). Certo non mancano anche storie realistiche, come quelle di Sciuscià ambientate nella Napoli del dopoguerra e pubblicate nel 1949 per i testi di Tristano Torelli e i disegni di Sacconi e Plaudetti, ma la tendenza di fondo resta quella esterofila.

11. È il formato 16 per 21 cm, per 96 pagine, brossurato e a costa, in bianco e nero. Tale formato sarà poi adottato dal figlio Sergio per tutti i fumetti seriali mandati in edicola dall'omonima casa editrice, che si affermerà gradualmente come la principale casa editrice di fumetti italiana. Cfr. G. BONEI, *I Bonelli. Una famiglia Mille avventure*, Milano 2017, Sergio Bonelli Editore.

gi western di successo quali il grande *Blek*, il Piccolo sceriffo e *Capitan Miki*, anche il popolare ranger cavalcherà essenzialmente negli Stati Uniti (soprattutto tra Arizona, Texas e New Mexico)¹².

Alla tendenza esterofila non saranno poi estranei neanche i cosiddetti «neri», usciti negli anni Sessanta nel più piccolo formato tascabile: *Diabolik* (creato dalle sorelle Angela e Letizia Giussani nel 1962), *Kriminal* e *Satanik* (creati nel 1964 dal duo Magnus & Bunker), e i molti loro epigoni in k¹³, che però continueranno a essere stranieri per nome e ambientazioni. L'innovazione sarà piuttosto sul piano dei contenuti, in quanto tali personaggi (che pur senza avere veri superpoteri hanno un'identità segreta e usano una calzamaglia) si smarcheranno nettamente dal modello positivo dei loro corrispettivi americani dell'epoca. Sono infatti ladri e assassini, pronti a usare tecnologia e abilità per scopi antitetici rispetto a quelli degli eroi tradizionali, così «facendo in mille pezzi, i tabù, la morale corrente, il bigottismo borghese e cattolico»¹⁴.

2. Gli unici prodotti a tiratura più ampia che presentino un'ambientazione di ispirazione almeno vagamente italiana sono personaggi di fantasia, rivolti ai più piccoli e dichiaratamente non realistici¹⁵. In ogni caso, la maggior parte dei personaggi umoristici del dopoguerra resta anch'essa ambientata in altri paesi¹⁶, ovvero agisce in ambienti non ben definiti o surreali¹⁷.

In questo quadro è interessante ricordare *Johnny Logan*, un personaggio minore e un po' trascurato dalla critica, realizzato tra il 1972 e il 1977 da Garofalo e Cimpellin, prima in formato tascabile e poi in albo poco più grande, per l'editoriale Dardo. Se è vero che – non a torto – è considerato una brutta copia dell'*Alan Ford* prima maniera, a differenza di quest'ultimo è apertamente italiano¹⁸ e italiano è il contesto in cui opera. Un contesto certo estremizzato, ma che pesca molti spunti dalla cronaca di quegli anni. Vengono così affrontati temi di attualità come il tentativo di colpo di Stato, il divorzio, la mafia, l'austerità e l'impopolarità dei politici.

Restando sul fumetto mainstream non sono mancate storie ambientate in Italia (come le avventure italiane di *Topolino*, *Martin Mystère*, *Alan Ford*). A ben

12. Americani saranno anche *Zagor* e *Mister No*, personaggi creati nel 1961 e nel 1975 dal figlio di Bonelli, Sergio, con lo pseudonimo di Guido Nolitta.

13. *Zakimort*, *Fantax* (divenuto poi *Fantasm*), *Mister-X*, *Sadik*, *Spettrus*, *Infernal*, *Demoniak*, *Samantha*, *Spiderman*, *Killing*. Anche la Disney italiana attingerà al genere con *Paperinik* (1969) e *Paperinika* (1973). L'unico che resterà in edicola fino ai giorni nostri sarà *Diabolik*.

14. G. SPONZILLI, *op. cit.*

15. Si pensi a *Soldino* e *Nonna Abelarda* (partoriti nel 1957 da Giovan Battista Carpi), *Cucciolo* (creato nel 1940 da Pedrocchi e Rino Anzi), *Tiramolla* (inventato da Roberto Renzi e Giorgio Rebuffi nel 1952), una parte della produzione di Jacovitti e in anni più recenti la *Pimpa* (frutto di Francesco Tullio-Altan nel 1975).

16. Ad esempio *Alan Ford* (di Magnus e Bunker, 1969) è basato a New York.

17. Così le *Sturmtruppen* (striscia creata nel 1969 da Franco Bonvincini, in arte Bonvi), *Lupo Alberto* (creato da Silver nel 1973), *Joe Galaxy* di Massimo Mattioli (1978), *Arthur King* di Bartoli e Domestici (1993), e il già citato *Rat-Man* di Leo Ortolani (1989).

18. Fanno infatti parte del gruppo di scalcagnati «cacciatori di taglie» lo stesso Jonny Logan (*alias* Giovanni Loganetti, un Lando Buzzanca in calzamaglia), Ben Talpa (al secolo Benito Talponi) e Dan Muscolo (ovvero Danilo Muscolotti).

vedere, numerosi personaggi inventati o elaborati dalla Disney in Italia, e gli stessi membri del Gruppo Tnt, pur vivendo in America, dimostrano sul piano caratteriale numerosi tratti (e vizi) nazionali ¹⁹: la caratterizzazione che ne viene fatta dagli sceneggiatori nostrani rende Paperino il vero eroe italiano ²⁰. Quasi una sorta di nicodemismo nel fumetto italiano, per cui molti personaggi partoriti da nostri autori sono «in fondo» italiani anche loro, ma dissimulano la propria psicologia sotto vesti straniere, per ragioni di opportunità.

Arriviamo quindi alla seconda metà degli anni Ottanta, quando le riviste, dopo il successo dei venti anni precedenti, iniziano gradualmente a entrare in crisi, lasciando tutto lo spazio al fumetto di massa, che ne ha peraltro assorbito molte qualità, maturando un forte rinnovamento stilistico e contenutistico. Grazie anche al lancio di nuove testate, il fumetto mainstream, soprattutto bonelliano, ha finito così per dominare incontrastato tra le produzioni seriali italiane (assieme ai titoli della Disney Italia, rivolti però a un pubblico più giovane), ponendosi come erede della narrativa popolare da Salgari in poi.

Per quanto riguarda i protagonisti, gli eroi bonelliani continuano a perpetuare il canone esterofilo del dopoguerra, presentando personaggi stranieri, soprattutto americani ²¹, e comunque mai italiani. Un canone confermato anche dai personaggi di genere fantascientifico, horror e fantasy ²².

Insomma, fino al 2007 in casa Bonelli l'unico ad avere ascendenze italiane è *Napoleone* (De Carlo, creato da Carlo Ambrosini nel 1997), che può vantare un padre italiano e una madre francese, ma è cresciuto ad Addis Abeba e abita in Svizzera (le sue avventure hanno inoltre una dimensione onirica).

Di fatto, i primi fumetti di formato bonelliano con protagonisti italiani, saranno prodotti da case indipendenti a partire dagli anni Novanta ²³. Ma che si tratti di eccezioni lo conferma il fatto che anche altri bonellidi continueranno a proporre ambientazioni estere ²⁴.

19. L'idea di Federico Pedrocchi, a partire dal 1935, fu infatti quella di assorbire i canoni stilistici e comportamentali disneyani, attingendo però anche a taluni elementi della cultura italiana. Cfr. A. Tosti, *Topolino e il fumetto Disney italiano. Storia, fasti, declino e nuove prospettive*, Latina 2011, Tunué.

20. La fattucchiera Amelia, basata sul Vesuvio, per contro è un'invenzione americana.

21. Oltre ai già citati *Tex* e *Zagor*, sono statunitensi i protagonisti di *Comandante Mark*, *Mister No*, *Ken Parker*, *Martin Mystère*, *Nick Raider*, *Julia*, *Magico Vento*, *Saguaro*, *Brad Barron*, *Cassidy* e quelli della miniserie *Caravan*.

22. *Jonathan Steel* è australiano, *Brendon* è uno scozzese, il vero nome del fantasy *Dragonero* è Ian Aranill, quello di *Dampyr* è Harlan Draka, *Nathan Never* è un cittadino del mondo futuro di origini euro-americane, come pure *Gregory Hunter* e *Morgan Lost*, gli *Orfani* sono iberici, *Lukas* vive in un'imprecisata città (l'unico riferimento all'Italia è l'amica Bianca Roberti), *Gea* vive in una metropoli alternativa e *Lilith* è inqualificabile.

23. Lo studente universitario *Billiband* (pubblicato dalla Editrice Universo dal 1994 al 1995), la dj fiorentina *Desdy Metus*, *Santiago* (di Rocco Dozzini, uscito in soli tre numeri in formato pocket nel 1996), *ESP* di Michelangelo La Neve (uscito su *l'Intrepido* dal 1992 al 2005 e anche in 18 numeri editi da Universo pubblicità in formato bonelliano dal 1995 al 1997), in cui però è romana solo l'ambientazione.

24. *Lazarus Led* (inventato da Ade Capone nel 1992, per i tipi della Star Comics) è americano, *Samuel Sand* (di Giovanni Barbieri, Marco Abate e Antonio Sarchione, pubblicato nel 1996 sempre dalla Star Comics) è parigino, *Gordon Link* (di Gianfranco Manfredi, stampato nel 1991 dall'Editoriale Dardo) si muove in una location europea postmoderna ma con nomi tutti anglosassoni. La città di *Spraylitz* (di

3. La ritrosia a creare eroi italiani è stata ancora più forte nei casi in cui i nostri autori si sono cimentati a creare supereroi, un genere che da noi ha avuto in via generale poco successo²⁵. Fatta eccezione per l'*Uomo Blindato* (apparso in una sola storia nel 1940 sulle pagine del *Corriere dei Piccoli*, il cui protagonista si chiamava Spartaco Ferri), la prima genia di eroi e supereroi *made in Italy* vide la luce nel secondo dopoguerra²⁶, in linea con l'esigenza di ottimismo della ricostruzione. Il genere si diradò negli anni Cinquanta per riprendersi parzialmente dagli anni Sessanta in poi²⁷, con serie che però ebbero tutte breve durata. Si tratterà soprattutto di personaggi sprovvisti di superpoteri innati o acquisiti (alla *Superman*), come ad esempio l'*Asso di Picche*²⁸, scritto da Mauro Faustinelli e disegnato da Hugo Pratt (successivamente autore del celebratissimo *Corto Maltese*).

I personaggi apparsi in questi tre decenni nella quasi totalità dei casi continueranno ad avere identità americane o straniere (se non parzialmente aliene, nel caso dei fumetti di fantascienza). È inoltre curioso notare che saranno rari quelli dotati di veri e propri superpoteri, quasi che dalle nostre parti un connazionale strapotente non venisse considerato credibile²⁹.

Di fatto gli autori nostrani non sembravano capaci di interpretare le potenzialità di un genere che iniziava ad affermarsi anche da noi, con l'adattamento delle serie americane di *Superman* e *Batman* negli albeti pubblicati dalla Cenisio prima e con il boom dell'Editoriale Corno poi. Quest'ultima dal 1970 propose infatti i nuovi «supereroi con superproblemi» concepiti da Stan Lee e Dick Kirby per la Marvel. Nel giro di poco tempo, l'*Uomo Ragno*, *Devil* e poi i *Fantastici Quattro*, *Thor*, *Capitan America* e altre diventano testate ad altissima tiratura³⁰.

Luca Enoch, stampato a partire dal 1992 prima su l'*Intrepido* e poi come serie dalla Star Comics) avrà invece richiami sia al mondo anglosassone che alle città italiane.

25. G. SPONZILLI, *op. cit.*

26. In rapida successione apparvero: nel 1945 *Tanks L'uomo d'acciaio* (di Carlo Cossio), *Ciclone* (di Andrea Lavezzolo e Carlo Cossio), *Asso di picche* (di Mario Faustinelli e Hugo Pratt) e *Yorga* (di Gian Luigi Bonelli e Antonio Canale); nel 1946 *Misterix* (di Max Massimino Garnier e Paul Campani), *Mistero* (di Franco Donatelli e Leonello Martini), *Amok* (di Cesare Solini e Antonio Canale); nel 1947 *Mirko* (di Carlo e Vittorio Cossio) e *Roal*; nel 1948 *Razzo l'Uomo di plastica*; nel 1949 *Plutos* (di Gian Luigi Bonelli e Leone Cimpellin) e *Maskar* (di Gallieno Ferri); nel 1952 *Rex, lo sparviero del mare* (di Antonio e Vincenzo Chiomenti). *Lupo* (apparso nel 1945 per i testi e i disegni di Lina Buffolente) è invece uno dei primi personaggi italiani di fantascienza.

27. Nel 1960 *Junior* e *Atlas* (entrambi di Luigi Grecchi e Loredano Ugolini); nel 1961 *Radar* (di Tristano Torelli e Franco Donatelli); nel 1962 *Atomik* (di Luciano Secchi – alias Max Bunker – e Paolo Piffarerio); nel 1964 *l'Ombra* (di Hugo Pratt); nel 1965 *Atoman* (di Santo D'Amico e Roberto Diso) e *Barbel* (di Angelo Platania); nel 1966 *Super Women* (di Clelia Ferrario e Renato Frascoli) e *Makabar* (di Fiorentini/Pedrazzi e Mangiarano/Zufe); nel 1974 *Medium* (di Garofalo e Trevisin) e *l'Ombra* (per i testi di Alfredo Castelli e i disegni di Fernando Tacconi e Mario Tubbino).

28. L'*Asso di Picche* fu pubblicato da Urugno Comics Inc. Venice, società dei giovani autori così denominata in emulazione dei fumetti stampati oltreoceano per i militari americani allora di stanza in Italia, e da questi spesso distribuiti ai nostri ragazzi dell'epoca. Più volte ristampato, il personaggio ha avuto successo anche in Argentina.

29. Fanno eccezione a questa regola solo *Tanks*, *Misterix* (che deriva la sua invincibilità da un congegno atomico), *Razzo*, *Atlas*, *Junior*, *Radar* (alieno ispirato a *Superman*), *Atomix* (che deriva i suoi poteri da un'armatura, in questo anticipando *Iron Man*) e *Medium*, nonché i «neri» con superpoteri come *Atoman*, *Barbel* e *Super women*.

30. I personaggi Marvel, dopo una parentesi di chiusura per il fallimento della Corno e un rilancio a fine anni Ottanta, sono tuttora pubblicati dalla Panini di Modena.

Nel 1994, sulla scia della ripresa delle pubblicazioni dei supereroi Marvel in Italia, alcuni autori provarono a rilanciare supereroi made in Italy. Il tentativo più ambizioso è rappresentato dagli albi della Phoenix *Italia XXII secolo*, usciti a partire dal 1994 sotto il coordinamento di Daniele Brolli. Si tratta di un intero universo super-eroico, ambientato nell'Italia del 2173 e i cui protagonisti sono prevalentemente giovani italiani come Paolo Canale (*alias* Examen), coinvolti nel progetto sentinella, che combattono in città come Adriatica e Nova Roma. Fumetti in media di buona fattura, che tuttavia erano destinati essenzialmente alle «fumetterie» e che hanno rappresentato pertanto un'esperienza circoscritta e limitata. Sempre in quest'ambito editoriale, l'anno successivo vedranno la luce anche altri supereroi di buon livello, come *Gabriel* (di Riccardo Secchi e Alessio Becatti), *Il potere e la gloria* (di Ade Capone e Stefano Raffaele), e nel 1997 *Videomax* (di Graziano Origa e Carlo Ambrosini), i cui protagonisti tornano però a essere americani (o tedeschi, come nel caso di *Videomax*)³¹. Sempre internazionali saranno poi i protagonisti delle miniserie *Euroforce* e *Gemini* della Marvel Italia, realizzata da autori prevalentemente italiani (come Giorgio Lavagna e Francesco Meo) così come quelli dei volumi *Quantum Academy*, prodotti a partire dal 2016 da Luca Baino e Lorenzo Susi, in collaborazione con la Scuola Internazionale di Comics.

Italiani saranno invece alcuni personaggi che vedranno però la luce fuori dal mercato delle edicole e avranno di conseguenza una diffusione ridotta: i fumetti concepiti da Fabrizio de Fabritiis per la casa editrice Emmetre Service (a partire da *Capitan Novara*³²), *Capitan Padania* (apparso nel 2006 nel solo numero *Padania libera*), Violet (supereroina antiamorrea creata da GG studio sul sito di *Repubblica* – Napoli nel 2016), il gruppo *Capitani Italiani* (concepito da Fabrizio Capigatti e altri autori inizialmente in autoproduzione e poi pubblicato dalla casa editrice da loro fondata Venezia Comics)³³, *Angie*³⁴ (fumetto lanciato nell'estate 2018 dalla Panini, la cui giovane protagonista Angie Digitwin si muove tra dimensione reale e digitale sullo sfondo di Torino, Milano e Roma³⁵).

Non mancheranno caricature del supereroe americano: il cyborg Ranxerox (creato da Stefano Tamburini e Tanino Liberatore nel 1978 sulla rivista underground *Il Cannibale*), il super-masochistico Ramarro (partorito da Giuseppe Pa-

31. Ambientazioni internazionali avranno anche altri tentativi usciti nel 1994: *Brain Trust* (testi di Stefano Sacco e Roberto Olivi e disegni di Paolo La Manna), *Dark side*, *Asmodeus* (di autori vari) e *Dept. H* (di Ade Capone, Paolo La Manna e Ivan Ibraini), uscito nel 1997, ma anch'esso effimero. L'unico a essere collocato nell'Italia (del futuro) sarà il mediocre *Antebac 20.87* (di Claudio Chilenni e Salvo Moscat).

32. *Capitan Novara*, al secolo Luca Ferrari, verrà pubblicato a partire dal 2004 su tovagliette pubblicitarie, in episodi a tavola unica. Seguirà lo spin-off *Romabot Centurion*, dedicato a un robot del futuro protettore dell'Urbe, e il progetto *Defenders of Europe*, supereroi provenienti dai diversi paesi europei (Russia inclusa).

33. Dopo un inizio nel 2006, nel 2012 *Capitan Venezia* è stato oggetto di un restyling e gli sono stati affiancati *Capitan Palermo*, *La Lupa* (protettrice di Roma) e *Capitan Napoli*.

34. Da un'idea di Luca Josi e Stefano Feltri, sviluppata da BS&M. I primi numeri sono stati scritti da Stefano Vietti e disegnati da Luca Enoch, Mario Alberti e Giancarlo Olivares.

35. Ambientazione solo in parte italiana avranno le storie a fumetti del progetto Timed, lanciato dalla Shockdom nel 2017. Un tentativo letterario è rappresentato dal romanzo di Max Gobbo *Capitan Acciaio. Supereroe d'Italia*, edito da Psiche e Aurora nel 2011.

lumbo nel 1986 sulla rivista *Tempi Supplementari*³⁶, il macchiettistico e più popolare Rat Man (creato da Leo Ortolani nel 1989, con fortunate edizioni anche seriali in edicola fino al 2017), il futuristico milanese trash Bravado di Diego Cajelli, Andrea Vogliono e Gianluca Maconi (pubblicato sul supplemento *Alias Comics* del *Manifesto* nel 2017), l'erotica *Super Tits* di Elena Mirulla (edito da Cronaca di Topolinia nel 2017), il satirico *Mecha Guevara* scritto e disegnato da Andrea Tridico e pubblicato da Manfont nel 2018, che vedrà il mitico Che tornare alla vita nel 1984 (grazie alla tecnologia sovietica) sotto forma di potente robot (appunto un *mecha*, alla giapponese)³⁷.

Dopo *Capitan Italia* (una parodia nostrana di Capitan America concepita da Walter Venturi e Stefano Piccoli, apparsa tra 1994 e 1998³⁸ e tra i cui nemici figura Euroman) l'esperimento più interessante vede la luce nel 2011: si tratta di *Primo*, fumetto pubblicato nel 2011 da BD Press con testi di Marco Rizzo e disegni di Lelio Bonaccorso. L'opera, assai originale, descrive una specie di Capitan America de noantri, concepito da uno scienziato fascista che non fa in tempo a compiere imprese eroiche durante la guerra, ma che viene risvegliato nel 1969. Dopo essere invischiato nel tentativo del colpo di Stato (mancato) del principe Borghese, il mascelluto protagonista rimbalzerà nel passato recente per diventare la prosaica guardia del corpo di un presidente chiamato «papy» dalle sue svenevoli ospiti.

Insomma: se negli anni in Italia si è sviluppata una tradizione super-eroica di una certa consistenza³⁹, fino alla prima metà degli anni Duemila questa non ha però vinto la sfida della durata (l'unico personaggio durato quasi trent'anni è il parodistico *Rat man*) e – con rare eccezioni – non ha infranto il tabù dell'eroe straniero.

4. Tornando indietro nel tempo, qualche spazio per personaggi italiani era stato offerto anche dal fumetto d'autore, pubblicato a partire da metà degli anni Sessanta su riviste di formato più grande e rivolte a un pubblico più maturo⁴⁰. Su queste riviste di nicchia appariranno infatti alcuni personaggi propriamente italiani, come il bolognese Zanardi (e i suoi cugini Pentothal e Pompeo, sempre di Andrea Pazienza), specchio del mondo underground e del movimento del Settantasette⁴¹, la milanese Valentina Rosselli di Guido Crepax, il detective bolognese Sam Pezzo

36. Sempre Palumbo, in coppia con Sebastiano Vilella, concepirà *Il mitico operaio*, con minore fortuna editoriale.

37. Il redivivo eroe rivoluzionario si scontrerà prima con Margaret Thatcher (*Iron Lady*), e poi con Ronald Reagan e la sua combriccola (protetta dal filtro antiideologico delle più grandi menti del liberalismo classico). Infine, al momento del confronto con la «progenie digitale» (che punta a creare una realtà dominata dalla Cartaleggio associati), si deciderà a eliminare il proprio sistema di autocensura (Pravda) che ne condizionava i comportamenti, liberando la satira.

38. Parodistico (e ambientato in Italia) è pure *Il Massacratore* di Stefano Piccoli e altri (apparso prima su fanzine e poi in edicola, a partire dal 1993).

39. «Asso di Picche – Supereroi all'italiana», n. 28 della serie *100 anni di Fumetto italiano* pubblicata da *Gazzetta dello Sport* e *Corriere della Sera* nel 2010.

40. Ad aprire la strada è *Linus* nel 1965, a cui negli anni successivi faranno seguito numerose altre.

41. Cfr. L. RAFFAELLI, «Quando la realtà cambiò il volto del fumetto», su *Fumetto italiano. Cinquant'anni di fumetti disegnati*, Ginevra-Milano 2016, Skira.

di Vittorio Giardino, alcuni personaggi di Manara e pochi altri⁴². Tra gli anni Ottanta e Novanta seguiranno Rudi X (pubblicato a partire dal 1987 sulla rivista *Comic Art*, per i testi di Rinaldo Traini e Giorgio Pedrazzi e i disegni di un team di autori di alto livello, basato a Roma ma perenne giramondo), nonché le storie genovesi di Giuli Bai & co (di Berardi e Milazzo, apparse a partire dal 1990 sempre su *Comic Art*) e quelle di Piera degli Spiriti di Mattoli e Toffolo (pubblicate sull'effimera rivista *Dinamite* della Granata Press nel 1995). Il più noto personaggio pubblicato su rivista, tuttavia, il *Corto Maltese* di Hugo Pratt, appare molto globalizzato per ambientazioni e per natali, avendo per genitori un marinaio della Cornovaglia e una zingara di Siviglia.

Su riviste a diffusione più giovanile e più ampia vi sono poi le interessanti esperienze del commissario Spada⁴³, l'adolescente Stefi⁴⁴ e il procuratore legale Lea Martelli⁴⁵, che restano però minoritarie, senza fare scuola, così come sarà un caso a sé la *Storia d'Italia a fumetti* scritta da Biagi⁴⁶.

Un vero e proprio cambio di registro si ha negli anni Duemila con nuove case editrici come Becco Giallo⁴⁷, che aprono la strada al *graphic journalism*⁴⁸ e al cosiddetto fumetto civile⁴⁹. A loro si deve infatti la pubblicazione di volumi con una forte apertura alla realtà italiana⁵⁰, commercializzati attraverso nuovi negozi specializzati (le fumetterie) e le tradizionali librerie. Opere singole che si concentrano su personaggi e vicende storiche e di cronaca come il sequestro Moro, le uccisioni di Ilaria Alpi, Peppino Impastato, Mauro Rostagno, le biografie di Falcone e Borsellino, don Peppe Diana, Enrico Mattei, don Milani, la morte di Federico Aldovrandi, le stragi di Portella della Ginestra, Bologna, Brescia, Piazza Fontana e Ustica, il massacro del Circeo, il mostro di Firenze, Unabomber, la scomparsa di Emanuela Orlandi, gli incidenti a Marcinelle, alla ThyssenKrupp, quello ferroviario a Livorno, il Vajont, il G8 di Genova, altri temi come l'inquinamento a Porto Marghera, Mani

42. Un caso a sé è *Poema a fumetti* di Dino Buzzati, pubblicato dalla Mondadori nel 1969 e considerato assieme a *La ballata del mare salato* di Hugo Pratt (uscita inizialmente a puntate) il primo graphic novel italiano. Pur partendo da un contesto milanese contemporaneo e riflettendo molti umori dell'epoca, *Poema a fumetti* ha essenzialmente un tratto onirico, ispirato al mito di Orfeo e Euridice.

43. Serie pubblicata sul *Giornalino* dal 1970 al 1982, per i testi di Gian Luigi Gonano e i disegni di Gianni De Luca. Ha descritto il nostro paese negli anni Settanta, coprendo anche temi come il movimento studentesco e il terrorismo.

44. Disegnato e scritto da Grazia Nidasio dal 1976 al 1992 sul *Corriere dei Piccoli*.

45. Creata da Cinzia Ghigliano e Marco Tomatis, e pubblicata sul settimanale femminile *Amica* dal 1977 in poi, ritrae un procuratore legale nello studio di un avvocato di provincia.

46. Un filone che anni dopo sarà ripreso da Ambrosini, Artibani, Milazzo e Toppi con 150 storie d'Italia, pubblicato da *Il Giornalino* in due volumi per il 150° anniversario dell'Unità d'Italia.

47. Creata nel 2005, questa casa editrice ha ripreso il nome della rivista antifascista *Becco giallo* del 1924.

48. In anticipo sui tempi, si può ricordare il reportage *Nicaragua 1984* pubblicato da Riccardo Mannelli nel 1985 da Giorgio Sestili Editore, che dimostrò le potenzialità di questo tipo di narrazione-inchiesta. Più di recente, il massimo interprete del genere è invece Gianluca Costantini, autore di *Fedele alla linea: il mondo raccontato dal graphic journalism* (2017). Per un esempio del suo approccio si può guardare questa presentazione dedicata alla divisione di Cipro, per i testi di Elettra Stamboulis.

49. Definizione coniata dal giornalista dell'Unità Renato Pallavicini. Cfr. F. FASIOLO, *Italia da fumetto. Graphic journalism e narrativa disegnata nel racconto della realtà italiana di ieri e di oggi*, Latina 2012, Tunué.

50. Per Federico Zaglio, uno dei tre editor di *Il Becco Giallo*, «la tendenza a raccontare la realtà si respirava nell'aria» (P. GIUDICI, «C'è chi ci mette il Becco Giallo», in *Annuario del Fumetto 2008*).

Pulite, la guerra civile dopo la liberazione, le foibe, la deportazione degli sloveni nel 1942-43, la campagna di Russia dell'Armir, fino a questioni più trasversali come l'emigrazione clandestina, la mafia, l'inquinamento dell'ambiente.

I nuovi editori⁵¹ daranno spazio crescente anche ai *graphic novel*, con storie di taglio biografico e tendenzialmente non seriali, sempre con una credibile collocazione nel Belpaese⁵². Tra i migliori esempi di romanzi grafici di questo tipo ricordiamo *5 è il numero perfetto* (di Igort, 2002) situato nella Napoli degli anni Settanta, *Solo andata* di Piero Macola (2005) che descrive l'Italia allo sbando dopo lo sbarco alleato in Sicilia del luglio 1943⁵³, *Morti di sonno* (di Davide Reviati, 2009) ambientato nel villaggio Anic di Ravenna, *Cinquemila chilometri al secondo* (di Manuele Fior, 2010) che tratteggia un delicato triangolo amoroso e d'amicizia tra provincia italiana, Norvegia e Egitto, il pittorico *Nottetempo* (di Luca Russo), che declina l'elaborazione di una perdita tra i malinconici sfondi di Venezia e del Museo di Capodimonte⁵⁴. Il miglior cantore della provincia (ricreata) è poi senza dubbio Gipi (alias Gianni Pacinotti). Zero Calcare, infine esplora con grande capacità temi autobiografico-generazionali di impegno civile, a partire dall'angolo visuale della propria *Heimat* di Rebibbia, nella periferia romana. Sia Gipi che Zero Calcare sono stati finalisti del Premio Strega (rispettivamente nel 2014 e nel 2015).

Certo la diffusione di queste opere rimane confinata soprattutto a fumetterie e librerie, rivolgendosi a un pubblico di nicchia, quantunque relativamente ampio (con l'eccezione di Zero Calcare, che ha tirature altissime, da edicola). Ma il terreno sembra in ogni caso ormai pronto per il lancio di nuovi eroi italiani, non solo autoriali ma anche di stampo popolare.

Da fine anni Novanta, questa nuova disponibilità del pubblico per personaggi italiani è comprovata anche dalla proliferazione di investigatori nazionali nella narrativa, da Montalbano in poi. La tendenza va di pari passo con il consolidamento di una fiction televisiva con positivi eroi italiani (spesso gli stessi della carta stampata)⁵⁵, protagonisti di serie con un identico schema di base, proprio come il fumetto popolare. I nuovi eroi del *noir* italiano sono spesso legati a realtà locali/re-

51. Ricordiamo case come Coconino Press, Edizioni BD, Minimum Fax, Edizione BD/Alta fedeltà, Kappa edizioni, Coniglio, Free Book, Canicola, Bao publishing, Round Robin, ReNoir, Shockdom.

52. P.L. GASPA, «Il romanzo grafico e l'avventura della storia», in *Fumetto italiano. Cinquant'anni di fumetti disegnati*, Ginevra Milano 2016, Skira.

53. Il ventennio fascista e la resistenza sono i periodi a cui sembrano essersi maggiormente ispirati i nostri autori. Tra i lavori ambientati in questo periodo si ricordano *Il maestro* di Andrea Laprovitera e Davide Pascutti (Tunué, Latina, 2008), *In Italia sono tutti maschi* di Luca De Sanctis e Sara Colaone (Bologna 2008, Kappa Edizioni), *Nessun ricordo* di Giovanni Marchese e Luca Gregorio Patané (Latina 2009, Tunué), *La porta di Sion* di Walter Chendi (Milano 2010, Edizioni Bd), *L'inverno d'Italia* di Davide Toffolo (2011), *L'inverno di Diego* di Roberto Baldazzini (2013) e *L'illusione della terraferma* di Otto Gabos (2015).

54. Dedicato al dramma del terremoto nell'Italia centrale e alla difficile ricostruzione è invece *La zona rossa*, di Silvia Vecchini e Antonio «Sualzo» Vincenti (Milano 2017, ed. Il castoro).

55. Pochi invece i film ispirati a fumetti italiani. Oltre a quelli tratti dai «neri», ricordiamo *Baba Yaga* del 1973 (ispirato a *Valentina* di Crepax), *Sturmtruppen* del 1976, *Tex e il signore degli abissi* del 1985, *Dylan Dog – Il film* (una produzione americana del 2010).

gionali, ma non per questo appaiono meno nazionali. Italiano è infatti il contesto storico in cui sono immersi (contemporaneo o meno)⁵⁶.

Sempre sul fronte cinematografico viene poi tentato un esperimento ancor più ambizioso: presentare non eroi, ma veri e propri supereroi italiani. Non che fossero mancati in passato alcuni tentativi: dalla trasposizione dei fumetti neri di fine anni Sessanta⁵⁷ alla saga di *I fantastici tre Supermen* (che ebbe un discreto successo, anche all'estero, tra il 1967 e il 1986, ma che rappresentava essenzialmente una parodia dei supereroi americani⁵⁸), passando per l'originale film di Bruno Bozzetto *Vip, mio fratello superuomo* (1968). Negli ultimi anni, tuttavia, anche a seguito del successo riscontrato in Italia dai film Marvel, vi sono stati due nuovi tentativi.

In *Il ragazzo invisibile*, diretto nel 2014 da Gabriele Salvatores, lo schema di base degli eroi Marvel (acquisizione di superpoteri apparentemente casuale, contrasto tra grandi poteri e grandi responsabilità che lacera interiormente il protagonista) viene applicato all'adolescente triestino Michele Silenzi, con un risultato complessivo dignitoso ma che non convince pienamente.

In *Lo chiamavano Jeeg Robot* dell'esordiente Gabriele Mainetti (2016), l'ambizione è molto superiore: non si tratta solo di applicare lo schema di Stan Lee a un ambiente italiano, ma di incrociare l'intuizione geniale dell'autore americano con uno sguardo realistico e non condiscendente sulle periferie e sulle marginalità nostrane, pescando protagonisti e antagonisti tra ragazzi di vita cresciuti in degradate borgate romane. Una riuscitissima sineddوحة tra Stan Lee e Pasolini⁵⁹. Ne esce «una storia impossibile con personaggi reali», con un supereroe socialmente e psicologicamente credibile⁶⁰. Pur con un budget oltre cento volte inferiore a quello di *Avengers*, il prodotto è ottimo (grazie anche alla strepitosa interpretazione di Luca Marinelli)⁶¹. Prova ne è che nel tragico finale il protagonista Enzo Ceccotti, uomo marginale e asociale divenuto super-forte grazie a un tuffo involontario nel limaccioso e radioattivo Tevere, accetta la propria maschera e il pro-

56. Diversi di questi personaggi verranno poi trasposti in fumetti, come l'*Ispettore Coliandro* (1994) e il *Brigadiere Leonardi* (2010), entrambi creati da Carlo Lucarelli, mentre Bonelli ha iniziato a pubblicare nel 2017 i begli adattamenti delle inchieste del *Commissario Ricciardi* ambientate nella Napoli degli anni Trenta. *Cacciatori nelle tenebre* può invece essere considerato uno spin-off dei romanzi di Carofiglio di cui è protagonista l'avvocato Guerrieri, che infatti vi compare brevemente. L'osmosi tra letteratura noir e fumetti è provata anche da *Cattivi soggetti – Il noir italiano a fumetti*, antologia coordinata da Daniele Brolli e dedicata a storie di immigrati in Italia (Milano 2010, Bur).

57. Si pensi a *Kriminal* (diretto da Umberto Lenzi nel 1966, e che ebbe un seguito due anni dopo), *Satanik* (di Piero Vivarelli, del 1968) e *Diabolik* (dal maestro horror Mario Bava, del 1968). A questo filone possono essere ascritti anche *Mister X* (di Piero Vivarelli, 1967) e *Flashman* (diretto da Mino Loy nel 1967). *Arriva Dorellik* (di Stefano Vanzina, 1968) è invece una parodia del genere.

58. Altri esempi sono *Goldface – Il fantastico superman* (girato nel 1968 da Bitto Albertini), *Superargo contro Diabolikus* (diretto nel 1966 diretto da Nick Nostro), seguito da *L'invincibile Superman* (diretto da Paolo Bianchini nel 1967). Più tardi seguiranno *Super Andy* – il fratello brutto di Superman (diretto da Paolo Bianchini nel 1979) e *l'Uomo puma* (di Alberto De Martino, del 1980). Infine si ricorda *Capitan Basilico* (di Massimo Morini, del 2008), seguito da *Capitan Basilico 2 – I Fantastici 4+4*, uscito nel 2011.

59. A. LEVANTESI KEZICH, «Accattone, ma dai superpoteri», *La Stampa*, 25/2/2016.

60. M. GOMARASCA, «Intervista a Gabriele Mainetti», *Nocturno.it*, 19/2/2016; G. CANOVA, «Tra schermo e vignetta», in *Otto e mezzo*, dicembre 2014.

61. R. NEPOTI, «Hollywood trema. Il supereroe ora è italiano», *la Repubblica*, 7/12/2017.

prio ruolo, diventando protettore del popolo romano. Un eroe romano e popolare fino al midollo, ma al contempo universale⁶².

5. In questo brodo di coltura nazionale, ormai aperto anche a una visione non solo parodistica⁶³, nel 2007 anche la Sergio Bonelli Editore si decide a pubblicare il primo fumetto seriale autenticamente italiano: si tratta di *Volto Nascosto*, uscito tra l'ottobre 2007 e il novembre 2008 con testi di Valerio Manfredi, artista versatile che recupera in modo originale l'esperienza coloniale italiana⁶⁴. Protagonista è l'italianissimo Ugo Pastore, giovane rappresentante di commercio che si muove tra Roma e l'Abissinia tra il 1889 e il 1896, fino alla disfatta di Adua⁶⁵. Il protagonista non è immune dalle caratteristiche tipiche di tanti eroi della letteratura italiana: pur vivendo in anni contrassegnati da un forte nazionalismo, Pastore è un idealista che comprende (e rispetta) le ragioni del nemico abissino, arrivando a dire «la mia Patria è il mondo»; inoltre, pur facendo un uso assai gagliardo della pistola, è allergico alla violenza gratuita. Manfredi riprende quindi il modello lanciato da Sergio Bonelli (che con Mister No aveva creato un personaggio molto umano⁶⁶, lontano dal modello un po' manicheo del paterno Tex⁶⁷) e lo cala in un contesto compiutamente italiano. Per molti versi è anche lui un minimalista, un antieroe, alla stregua del Carlo Altoviti di *Confessioni di un ottuagenario*.

Negli ultimi anni, le concorrenti della Bonelli pubblicano altre miniserie ambientate nell'Italia contemporanea, che però hanno un corto respiro editoriale⁶⁸. Tra queste spicca *Valter Buio*, pubblicata da Star Comics, il cui protagonista (Dottor Buio) è psicanalista dei fantasmi che opera nella Roma contemporanea. L'autore, Alessandro Bilotta, è uno sceneggiatore che ha come tratto distintivo (sin

62. Entrambi i film sono stati oggetto di adattamenti a fumetti, ma mentre la versione di *Il Ragazzo invisibile* (realizzata da Diego Cajelli per i disegni di Giuseppe Camuncoli, Werther dell'Edera e Alessandro Vitti) sviluppa e integra la trama cinematografica, quella di *Lo chiamavano Jeeg robot* (scritta da Recchioni e disegnata da Giorgio Pontrelli e Stefano Simeone) rappresenta un sequel del film.

63. «La voglia di raccontare realtà non accenni a diminuire e anzi si riproponga come tratto dominante dei primi anni del XXI secolo», F. FASIOLO, *op. cit.*, p. 259.

64. A partire dal 2007 la SBE inizierà a pubblicare anche i *Romanzi a fumetti*, volumi autoconclusivi di 300 pagine alcuni dei quali accoglieranno storie nere ambientate in Italia.

65. Le avventure di Pastore sono poi proseguite con una nuova serie scritta da Manfredi (*Shanghai Devil*) che racconta del trasferimento del protagonista in Cina, con questa volta sullo sfondo la rivolta dei boxer.

66. Per molti versi *Mister No* è quindi un antieroe, come lo saranno poi altri successi della casa editrice, da *Ken Parker* a *Dylan Dog* e *Nathan Never*.

67. Secondo una lettura più articolata apparsa di recente, la caratterizzazione del ranger risponderebbe tuttavia alla duplice esigenza di superare le ostilità del post fascismo e affrontare la ricostruzione in modo pratico e urgente (E. LEAKE, *Tex Willer. Un Cowboy nell'Italia del dopoguerra*, Bologna 2018, il Mulino).

68. *Unità speciale – CC* (giallo dedicato alla Benemerita pubblicato per 15 numeri dal 2008 dall'Eura Editoriale, e poi trasferito su Skorpio), *Cornelio* (personaggio *horror* ispirato allo stesso scrittore Lucarelli, edito da Star Comics in 12 numeri tra 2008 e 2010), *San Michele* (miniserie in sei volumi pubblicata dalla Star Comics e ambientata in un borgo dell'Italia centrale a partire 2010), *Nuvole nere* (miniserie che raccoglie racconti di Lucarelli pubblicata sempre dalla Star Comics in sei volumi a partire dal 2011), *Davvero* (riuscito *shojomanga* uscito nel 2011 per la Star Comics e ambientato da Paola Barbato nella provincia padana), *Magnifico!* di Pietro B. Zemelo (nato nel 2013 come *strip online* e poi stampato da Manfont).

dagli esordi con la propria casa Montego) quello di ambientare in Italia le sue storie. Dal 2001, Bilotta aveva infatti scritto (con il disegnatore Carmine di Gandomenico) interessanti opere come *Le strabilianti vicende di Guido Maraviglia – inventore* (ambientato in una Roma alternativa del 1914), *La lande des aviateurs* (ucronia ambientata in un universo alternativo, che pur essendo pubblicata in Francia ha personaggi totalmente italiani), *Romano – Un automne de dix secondes* (storia sofferta di un pugile nella povera Roma del dopoguerra) e la splendida *La Dottrina*, un'inquietante distopia (edita da Magic Press nel 2003) che riprende la migliore tradizione della letteratura e del fumetto contemporanei, da *1984* di Orwell a *V per vendetta* di Moore e Lloyd⁶⁹. Anche qui abbiamo una società totalitaria e alienante, turbata dall'improvvisa irruzione di un ribelle, ma i protagonisti (e i comprimari) sono quasi tutti italiani: Zaccaria, Tea, Taddeo, Tonio, con qualche eccezione come Zhao (che comunque si fa chiamare Sasso). Italiani anche i ruoli principali dell'oppressivo sistema di governo: la guida suprema è «il Nocchiere», il burocrate di più alto livello «il Primate», le guardie sono «i professori», il ribelle è «la smorfia». I capitoli sono inframezzati da pagine della Dottrina Perelà, rimando diretto al romanzo futurista di Palazzeschi.

A fine 2016 Bilotta lancia con l'ammiraglia Bonelli la nuova serie *Mercurio Loi*, dedicata a un curioso pensatore e investigatore per diletto che si muove nella Roma papalina del 1826, a cui nel gennaio 2015 era stato dedicato un episodio *one shot* di *Le storie*, serie mensile con episodi autoconclusivi. Un progetto interessante e ambizioso, per un risultato molto apprezzato dalla critica e forse un po' meno dalle vendite (come sembra indicare il passaggio della periodicità da mensile a bimestrale). Le avventure del buon Mercurio indulgiano molto sulla riflessione filosofica più che sull'azione (il protagonista è sostanzialmente tollerato dalle repressive Autorità dell'epoca, pur apparendo *borderline* per il suo libero pensiero) e vi è poca traccia delle tensioni nazionalistiche dell'epoca. Ma è una precisa scelta dell'autore, in quanto l'ambientazione storica deve restare semplice contesto in cui calare un'originale opera di fantasia, senza sovrastare i personaggi, che restano centrali⁷⁰.

Sempre per quanto riguarda la Bonelli, di recente avranno poi ambientazioni italiane anche alcuni numeri di *Le storie*⁷¹, alcuni *one shot* lunghi⁷², nonché episodi di serie come *Julia* (da ultimo il n. 238 «Milano calibro 7.65»), *Martin*

69. Diverse opere significative dei nostri fumettisti sono ucronie/distopie ambientate in Italia. Oltre al già menzionato *Rankxerox*, si possono ricordare *Napoli Ground Zero* del collettivo di autori che ruotava attorno a Roberto Recchioni e a Lorenzo Bartoli (Napoli 2003), *Appunti per una storia di guerra* di Gipi (2005), *Brodo di niente* di Andrea Bruno (2007), *La neve se ne frega* di Matteo Casali e Giuseppe Camuncoli tratto da un romanzo di Ligabue (2008), *United we stand* di Simone Sarasso e Daniele Rudoni (2009), *Kannonau – Fortza Paris*, scritto da Roberto Di Leo e disegnato da Andrea Tivellini (2018). In questo quadro non mancano distopie italiane prodotte all'estero come *Imperator – Les fascistes sont éternels* di Valérie Mangin e Fafner (2012).

70. Intervista a A. BILOTTA, *Scuola di fumetto* n. 106, maggio-giugno 2017).

71. Ad esempio il n. 70, *Leone*, scritto da Diego Cajelli e disegnato da Arjuna Susini e Francesco Francini.

72. Da ultimo *Sessantotto. Cani sciolti*, scritta da Gianfranco Manfredi per i disegni di Luca Casalan-guida.

Mystère (in particolare la bella recente miniserie «Le nuove avventure a colori»), e altri come *Dampyr* (ad esempio «Il segreto del bosco magico», in *Maxi Dampyr* n. 1, agosto 2009).

Ma è con Roberto Recchioni, autore poliedrico a suo agio come sceneggiatore e disegnatore ma anche come blogger ed editor di successo⁷³, oltre che punto di riferimento per numerosi nuovi autori, che giungiamo al culmine di quest'evoluzione. Già animatore dell'interessante esperimento *Napoli Ground Zero* nel 2003 e supervisore dieci anni dopo di *Long Wei* (il cui protagonista è un cinese trasferitosi a Milano, nella Chinatown di via Paolo Sarpi)⁷⁴, nel 2014 Recchioni decide di rilanciare un proprio vecchio personaggio, il vampiro siciliano Pietro Battaglia. Quest'ultimo, concepito nel 1994 come uno dei membri della squadra di Dark Side⁷⁵, era stato messo a punto alcuni anni dopo con il disegnatore Leomacs nelle storie *Vota Antonio* (ambientate nella campagna elettorale del dopoguerra in Basilicata, con atmosfere tra Guareschi e Leone) e *Le guerre di Piero – Caporetto* (che definisce la genesi del personaggio). Si tratta di un personaggio tipicamente italiano, anzi siciliano, quindi italianissimo. Pietro (il nome è un probabile omaggio a *La guerra di Piero* di De André), è infatti un soldato semplice che durante la grande guerra soffre e combatte, sognando di tornare dalla sua Ninetta. Perde la vita a Caporetto (momento a suo modo fondativo dell'identità nazionale), ma quando la morte gli appare sotto forma di una bella mora che gli propone il classico patto col diavolo, lui rifiuta, venendo così condannato all'immortalità. Un'immortalità che verrà trascorsa in gran parte in Italia.

A partire dal 2015 Recchioni rilancia Battaglia in una miniserie (pubblicata dall'Editoriale Cosmo prima in formato tascabile – come i «neri» di un tempo – e poi nel più convenzionale formato Bonelli). Questa volta il vampiro siciliano attraversa emblematiche vicende nazionali dal fascismo in poi (il G8 di Genova, il ventennio, il sequestro Moro, mafia, camorra e nuova criminalità cinese, il delitto Pasolini, la strage di Ustica, le foibe, la scomparsa di Moana Pozzi, Padre Pio, l'ascesa e il declino di Berlusconi), dando libero sfogo al proprio abissale cinismo di fronte alle ricorrenti collusioni tra Stato, Chiesa e malavita, di cui si presta peraltro a essere la sporca mano. Se Diabolik vive in un universo assurdo (un mix tra Svizzera, bassa padana, Inghilterra e Stati Uniti), Battaglia vive in

73. Dopo aver esordito nel 1993 con la serie *Dark Side* (edita da B.D. Press e orgogliosamente sotto-titolata «Fumetto italiano») e fondato assieme ad altri la casa indipendente Factory, Recchioni ha collaborato con i principali gruppi editoriali italiani. Tra le sue produzioni si ricordano le serie *John Doe* e *Detective Dante* (create con Lorenzo Bartoli per l'Editoriale Eura), la miniserie *David Murphy – 911* (realizzata con Matteo Cremona per Panini Comics nel 2008), la miniserie *Garrett – Ucciderò ancora Billy the Kid* (2007, Edizioni BD), i volumi *Asso* e *Ammazzatine* (2012, Nicola Pesce Editore), l'adattamento de *Le Cronache del Mondo Emerso* di Licia Troisi nel 2009, *Monolith* (pubblicato in due volumi nel 2017 e oggetto di una parallela versione cinematografica) e *La fine della ragione* (2018, Feltrinelli comics). È l'ideatore della collana *Roberto Recchioni presenta: i maestri dell'orrore* (Star Comics) e dal 2016 è curatore di *Dylan Dog*.

74. Scritto da Diego Cajelli e disegnato da Luca Genovese, *Long Wei* è stato pubblicato da Editoriale Aurea, in dodici volumi di formato bonelliano, a partire dal maggio 2013.

75. In questi albeti, scritti da Recchioni e disegnati da una serie di altri autori in stile vagamente manga, Battaglia si presentava inizialmente come una specie di Wolverine.

scenari assolutamente italiani, di ieri e di oggi. Antieroe (italiano) in tutto e per tutto, mette a nudo le maggiori ipocrisie nazionali. È un cattivo, certo, ma si confronta spesso con chi è più cattivo di lui.

Battaglia prosegue poi le sue avventure – questa volta come coprotagonista – nella serie *Caput Mundi* – *I mostri di Roma*, pubblicata sempre dalla Cosmo: 6 albi in formato bonelliano da 144 pagine, da novembre 2017 a febbraio 2018. La serie presenta un universo narrativo coerente e in *continuity* (come per i Marvel) che vede come protagonisti – oltre al succhia sangue Battaglia – altri mostri di vecchia e nuova generazione: lupi mannari (di Ostia), una donna fatale insensibile al dolore, un giudice anfibio che ricorda Swamp Thing, l'uomo invisibile e una mummia (però in abiti cardinalizi). Tutti italiani o italianizzati.

Caput Mundi, ispirato da un'idea di Roberto Recchioni e curato da Giulio A. Gualtieri (che aveva già collaborato con Recchioni alla serie *Caravaggio* edita su Skorpio e al bonellide John Doe, per Eura Editoriale), appare debitore anche delle serie televisive *Romanzo criminale* e *Suburra*: ormai anche l'Urbe attuale è di moda, sia pure come scenario negativo. Lo stesso Gualtieri scrive nell'introduzione al numero 5: «Hollywood attinge a piene mani dal mondo intorno a sé (...) Anche il re degli scrittori, il buon Stephen [King], non fa altro che raccontare di casa sua: il Maine. (...) Scrivi di quello che conosci. È questa la vera lezione della scuola narrativa Usa. (...) Così, la nostra America l'abbiamo trovata a Roma: (...) la città che conosciamo meglio».

6. La pluridecennale assenza di eroi autenticamente (e positivamente) italiani ha avuto varie spiegazioni. Le più diffuse sono storico-politiche: dopo l'ubriacatura fascista – con la sua pretesa di eroi italici e con risultati propagandistici e falsi – non vi era più spazio per personaggi nazionali; oppure, le culture dominanti della Prima Repubblica, vedendo contrapposti comunisti e filoamericani, non avrebbero dato spazio a eroi condivisi. Nemmeno la storia prefascista del nostro paese, Risorgimento incluso, si dimostrava sufficientemente consolidata e interclassista per costituire una base condivisa

Certo c'erano case editrici schierate: si pensi al *Vittorioso* prima e al *Giornalino* poi, di area cattolico-moderata, mentre il *Pioniere* faceva riferimento a quella comunista⁷⁶. Ma per editori neutrali come quella che sarebbe poi diventata la Bonelli era più comodo collocare i propri eroi in contesti americani, del passato o del futuro.

76. Se per l'area comunista (eccezion fatta per intellettuali come Vittorini), i pregiudizi rispetto ai fumetti americani erano spiegabili con ragioni di schieramento internazionale, la diffusione di tali pregiudizi anche nel mondo cattolico era invece ascrivibile al portato ritenuto potenzialmente antieducativo e immorale dei *comics* e dei fumetti in genere, tanto che nel corso della prima legislatura fu esaminato (e approvato dalla Camera) un disegno di legge in materia di censura su questo tipo di pubblicazioni, promosso dalla deputata democristiana Maria Federici. Complice il latente antiamericanismo diffuso nel nostro paese, anche nel dopoguerra i fumetti americani continuarono a essere sottoposti ad adattamenti (ben 150 le manipolazioni cui fu sottoposto Superman sugli Albi del falco editi da Mondadori a partire dal 1954, a partire dal cambio di nome in Nembo Kid, scelto «probabilmente per non urtare la suscettibilità di certi ambienti cattolici con accostamenti all'osteggiata filosofia del superomismo di Nietzsche»).

Un'altra tesi è legata alla grande influenza dell'immaginario e dei generi americani nell'Italia postbellica, dove non sarebbe stato possibile concepire protagonisti italiani di storie di fantascienza o western. Una tesi che convince a metà: nel caso del western, la lettura fatta dagli italiani (Sergio Leone, ma non solo) è spesso profondamente innovativa rispetto all'originale, tanto da diventare per molti versi un modello per gli stessi americani; inoltre, lo stesso cinema hollywoodiano si è spesso ispirato ad ambientazioni «italiche» (si pensi al successo dei *peplum*)⁷⁷.

Una tesi per molti aspetti opposta addita invece il conformismo storico nostrano, per cui in Italia predominerebbe «una concezione troppo ingessata e istituzionale della nostra storia, (che non consentirebbe di) raccontare (...) le avventure di Garibaldi con la stessa libertà e varietà di toni con cui gli americani hanno raccontato Custer o i francesi Napoleone»⁷⁸. Anche di questo ci consentiamo di dubitare, in quanto non sono mancate produzioni letterarie o cinematografiche assai critiche rispetto a passaggi importanti della nostra storia.

Certo è che da noi la sconfitta nella seconda guerra mondiale ha comportato un lungo e generale calo d'interesse per la storia nazionale, ripercossosi anche sulle diverse forme di narrativa. Da questo punto di vista, la «morte della Patria» avrebbe implicato anche la morte dei patrioti a fumetti per larga parte del secondo dopoguerra.

Paradossalmente, sarà proprio negli anni Novanta – anche a fronte di fenomeni politici come il primo leghismo e le opposte tendenze neoborboniche, uniti nel contestare le rappresentazioni tradizionali del percorso unitario – che comincerà a riemergere un interesse diffuso per la storia patria. Di qui nasce un percorso che ci ha portato a Battaglia e compagnia. Supereroi per molti versi negativi, anche se dopo le decostruzioni del modello americano operate da Frank Miller e Alan Moore a fine anni Ottanta è difficile proporre personaggi positivi che non siano didascalici, mentre la nostra tradizione realistica porta a diffidare di ciò che appare un po' finto. Una tendenza radicata anche nella nostra letteratura, che non ha prodotto veri eroi e non ha visto la sacralizzazione patriottica dei protagonisti di maggior successo⁷⁹. Sarà forse per questo che i fumetti più riusciti con protagonisti credibilmente italiani sono dedicati a personaggi «neri».

Certo, i personaggi italici di Recchioni & co. non hanno una diffusione di massa: le tirature della Cosmo, ancorché basate sulla distribuzione in edicola, sono infatti modeste e la conoscenza di Pietro Battaglia resta limitata nel grande pubblico. Ma occorre riconoscere che negli ultimi venticinque anni la diffusione del fumetto, soprattutto stampato, è calata drasticamente, soprattutto tra i più giovani, insidiata da Internet, videogiochi e serie tv⁸⁰. Oggi i fumetti (stampati) li leggono

77. Di converso, c'è chi ha osservato che essendo il supereroe una figura tipica della cultura americana, essa non avrebbe potuto essere replicata da autori italiani. Una tesi che potrebbe essere estesa anche al resto d'Europa.

78. P. GIUDICI, intervista a Gianfranco Manfredi, *Annuario del fumetto 2008*.

79. S. JOSSA, *Un paese senza eroi: L'Italia da Jacopo Ortis a Montalbano*, Roma-Bari 2013, Laterza.

80. Secondo Michele Masiero, «uno dei problemi del settore è "agganciare" le nuove generazioni distratte da Internet, YouTube, serie tv e videogiochi». Cfr di L. MARAGNO, «Cinema e fumetti made in Italy: chi sono i lettori di fumetti? Un identikit del lettore italiano di comics», *Best Movie*, 2/3/2017.

soprattutto gli adulti, anche attempati⁸¹.

Ciò non esclude tuttavia che Pietro Battaglia o altri personaggi come lui possa-
no raggiungere una diffusione molto maggiore. Anche in America il successo enor-
me dei film prodotti negli ultimi dieci anni dai Marvel Studios (tre di loro figurano
nella classifica dei 10 film con i maggiori incassi di sempre) non ha alcun rapporto
con le attuali tirature su carta degli omonimi eroi: se il film *Avengers* ha staccato
biglietti per oltre 1,5 miliardi di dollari, la serie a fumetti dedicata al super gruppo
continua ad aggirarsi tra le 40 e le 80 mila copie al mese (meno di quanto venda in
Italia *Dylan Dog*). Tanto che alcuni hanno osservato che il successo sul grande
schermo di *Thor*, *Capitan America* e compagnia non deriva tanto e solo dalle loro
matrici fumettistiche, quanto dalla loro natura archetipica⁸² che li fa risultare eroi
«naturalisti» in tutto il mondo, una volta trasposti in mega produzioni hollywoodiane.
Come ha osservato il docente di linguaggi audiovisivi Marco Stefanelli, «ciò che
colpisce maggiormente è la centralità culturale che il mondo del fumetto e i suoi
eroi continuano ad avere [nel] mondo dello spettacolo. (...) La sua forza sta nell'es-
sere un ponte tra l'universo della carta e quello visivo. (...) Le storie di supereroi
sono un'enorme *library* dell'immaginario a disposizione dei produttori»⁸³.

Chissà che ciò non avvenga un giorno anche per il vampiro siciliano e i suoi
fratelli.

81. Sull'evoluzione per certi versi paradossale per cui il fumetto contemporaneo sarebbe diventato una «forma di cultura alta», cfr. l'intervista a Umberto Eco apparsa sul *Manifesto* il 28 aprile 2011.

82. Secondo una consolidata tradizione, i supereroi sarebbero essenzialmente americani. In realtà un'analisi più approfondita rileva come le figure supereroiche più note abbiano una natura archetipica, riprendendo alcune figure mitologiche e anche religiose (e sciamaniche) presenti anche a livello europeo. M. ARNAUDO, *Il fumetto supereroico. Mito, etica e strategie narrative*, Latina 2010, Tunué; A. COCCIA, «Supersfortunato il paese che ha bisogno di supereroi», *L'inkiesta*, 6/4/2016.

83. F. FASIOLO, «I fumetti e il superpotere dell'eternità», *la Repubblica*, 29/9/2016.

ALESSANDRO ARESU - Consigliere scientifico di *Limes*.

JOHN BAMBENEK - Insegna Cibersicurezza presso la University of Illinois.

EDOARDO BORIA - Geografo presso il dipartimento di Scienze politiche dell'Università La Sapienza di Roma, è titolare degli insegnamenti di Geografia e di Geopolitica. Consigliere scientifico di *Limes*.

GIOVANNI COLLOT - Giornalista residente a Bruxelles, scrive di politica statunitense ed europea. Cofondatore di iMerica e direttore della lettera del lunedì del Groupe d'études géopolitiques.

MATTHEW CROSTON - Insegna Global security presso l'American Military University. Dirige *The International Journal of Intelligence and Counterintelligence*.

GIORGIO CUSCITO - Consigliere redazionale di *Limes*. Analista, studioso di geopolitica cinese. Cura per *limesonline.com* il «Bollettino imperiale» sulla Cina.

DARIO FABBRI - Giornalista, consigliere scientifico e coordinatore America di *Limes*. Esperto di America e Medio Oriente.

GEORGE FRIEDMAN - Fondatore e ceo di *Geopolitical Futures*.

ANDREA GHIZZONI - Direttore di WeChat Europa.

PRABHU GUPTARA - Insegna Global business, management e public policy presso la William Carey University.

JAMES LEWIS - Vicepresidente del Center for Strategic and International Studies.

NICCOLÒ LOCATELLI - Coordinatore (web e social media) di *limesonline.com*. Membro del consiglio redazionale di *Limes*.

LUCA MAINOLDI - Consigliere redazionale di *Limes*. Segue tematiche relative alla geopolitica e alla storia dell'intelligence.

FRANCESCO MASELLI - Giornalista, collabora con *L'Opinion*, *Il Foglio* e Radio24.

FRANK PASQUALE - Professore di Diritto presso la University of Maryland.

FEDERICO PETRONI - Consigliere redazionale di *Limes*, responsabile del Limes Club Bologna e cofondatore di iMerica.

SIMON TEMPLAR - Esperto in cibersicurezza e *fake news*.

PIETRO TINO - Professore associato di Storia contemporanea, insegna Storia sociale, Storia dell'agricoltura e Storia dell'ambiente presso il dipartimento di Studi umanistici dell'Università degli Studi Roma Tre.

FRANCESCO VITALI GENTILINI - Esperto nel campo della protezione dati in particolare nel settore dei big data, Information & Communication Technologies, studi strategici. Componente dell'Osservatorio sul contenzioso pubblico - Roma. È membro del Consiglio degli esperti del @LawLab - Laboratorio sul diritto del digitale presso l'Università Luiss-Guido Carli di Roma.

La storia in carte

a cura di *Edoardo BORIA*

Il ciberspazio è, in ordine di apparizione, l'ultimo tra i grandi teatri dello scontro geopolitico. L'hanno preceduto la terra e il mare, che erano gli spazi orizzontali della geopolitica classica, poi lo spazio aereo, che ha aperto a inizio Novecento alla terza dimensione, quella verticale, e infine lo spazio cosmico, che ha contrassegnato la guerra fredda. Ora è la volta del ciberspazio, quello virtuale della Rete e dei social che rende così originale il nostro tempo.

Ognuno di questi teatri prevede le proprie regole d'ingaggio e le proprie strategie di combattimento, impone vincoli e offre opportunità a soggetti inevitabilmente politici ma non per natura, come gli Stati, bensì per vocazione. Parliamo dei protagonisti della Rete mappati nella *figura 1*, dove ipotetiche linee della metropolitana rappresentano specifici ambiti di servizi online: linea «tecnologica» lungo la quale si colloca la fermata «Microsoft», linea «dei contenuti» dove si può scendere e salire a «Cnn» e così via. Le scritte delle fermate sono proporzionali al peso di questi giganti da cui prendono il nome.

Si noti, all'estremità in basso al centro, l'unico soggetto italiano ammesso a questo pantheon della Rete: il blog «BeppeGrillo». Eravamo solo nel 2007, ma l'esito politico di quel blog rende chiarissimo quanto il ciberspazio sia oggi non solo un nuovo spazio geopolitico che ridisegna le forme e l'esercizio del potere, ma forse addirittura la più importante dimensione della produzione del potere. Uno spazio in cui persino l'individuazione di un centro e di una periferia è costantemente in discussione, al contrario degli stabili spazi delle comunicazioni del passato quale quello della *figura 2*, il cui baricentro su Londra ne esalta la funzione incontrastata di *hub* del mondo.

Le caratteristiche del ciberspazio sono molto singolari se le si confronta con quelle degli altri quattro teatri: è l'unico non derivante dal mondo naturale ma completamente artificiale; è quello che ospita più regimi di proprietà, da quella privata a quella statale, da quella individuale a quella collettiva; è accessibilissimo con risorse minime anche a soggetti individuali, tanto che il computer è *personal* e l'hacker solitario una figura temuta; infine — e questa è la caratteristica più rilevante per la geopolitica che eleva lo scontro a regola, la conflittualità a condizione endemica della politica — le sue risorse sono illimitate e non esclusive.

Ne deriva l'impressione che la natura del ciberspazio sia quella di un sistema non gerarchico. Uno spazio liscio, uniforme, dove a tutti sono date le medesime opportunità. Illusione. Il grado di alfabetizzazione tecnologica e le disponibilità economiche ad accedere al mondo della Rete sono altamente differenziate. Stesso per la dotazione infrastrutturale tra le diverse regioni del pianeta, e anche all'interno di esse. Condizioni strutturali che esaltano le differenze, esattamente come avviene nelle comunicazioni terrestri, con cui il ciberspazio condivide la natura inevitabilmente discriminatoria della logica reticolare. Così, come sulla terra fa differenza se ci si sposta su un mulo, su un camion o in treno (*figura 3*), allo stesso modo l'efficienza dei percorsi della comunicazione in Rete dipende dalle capacità infrastrutturali delle dorsali. Ecco spiegato il *digital divide*, per cui solo un terzo del pianeta si connette effettivamente a Internet (dato riportato in M. VEGGETTI, *L'invenzione del globo*, p. 202). Altro che democrazia della Rete!

Come rappresentiamo il ciberspazio? Quale cartografia abbiamo sviluppato per raffigurarlo? Quale struttura spaziale esso assume? Qui sorgono dei problemi perché

non abbiamo un modello di rappresentazione. O meglio: quello che abbiamo – topografico-euclideo – non serve. La carta tradizionale, nata per raffigurare la superficie terrestre e dunque originariamente allestita per trasferire sulla carta oggetti fisici, visibili, materiali, entra in crisi quando le viene chiesto di passare a visualizzare oggetti dematerializzati, cioè entità invisibili o dotate di una spazialità liquida. C'è infatti una contrapposizione di fondo tra l'estetica naturale della carta razionalista, finalizzata a informare su una realtà tangibile, e l'estetica artificiale di una rappresentazione di Internet, limitata a trasmettere sensazioni su una realtà impalpabile. Ecco allora che, di quello spazio astratto, non riusciamo a raffigurare le fattezze ma solo a misurarne alcuni fenomeni quali, tipicamente, i contatti tra i nodi.

La figura 4 visualizza il traffico dati tra New York e altre 250 città del mondo in 24 ore. La grandezza dei simboli a forma di bagliore di luce è proporzionale al volume di traffico.

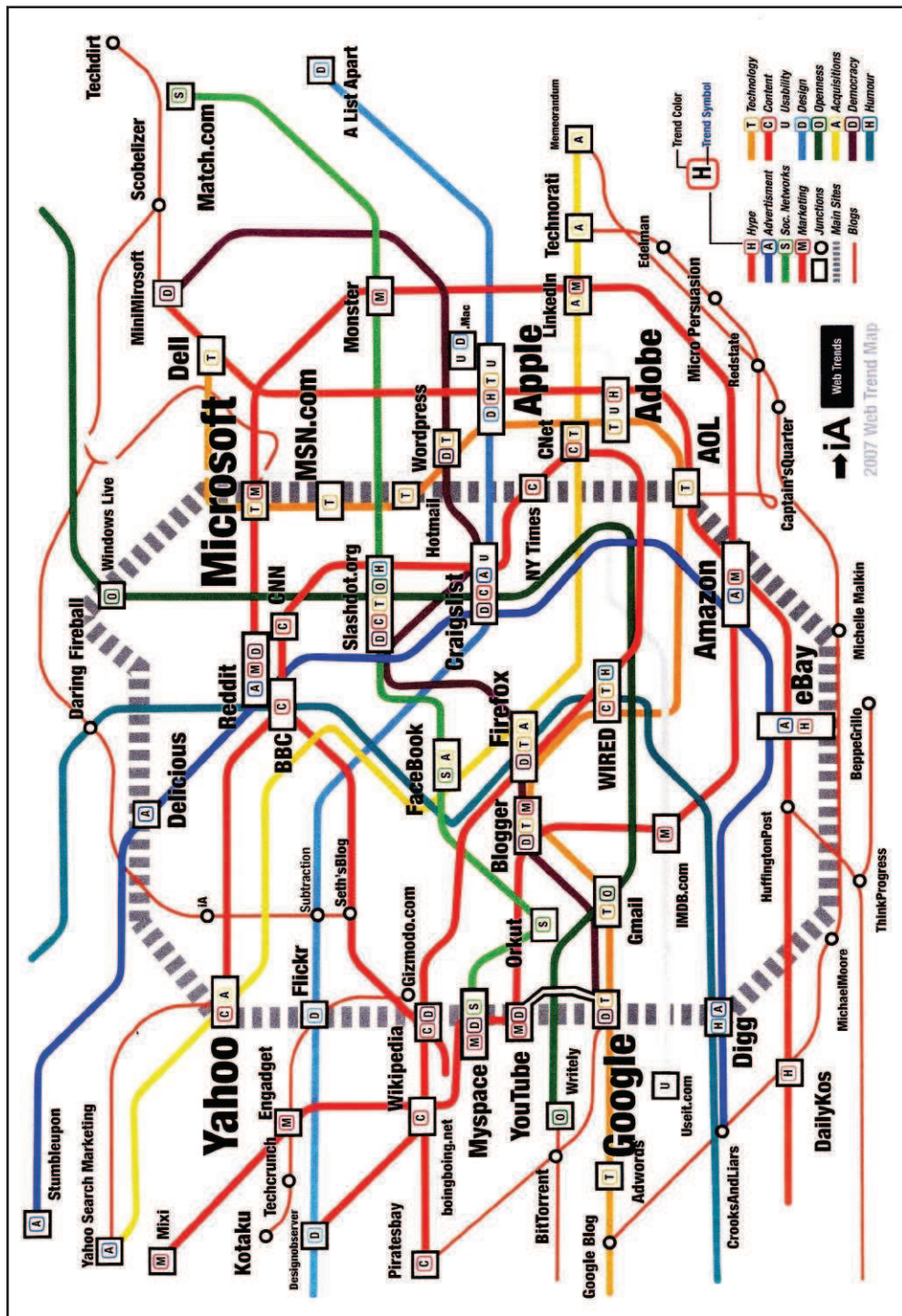
Le comunicazioni di oggi avvengono però in un contesto caratterizzato da una fortissima compressione spazio-temporale. Non che si tratti di un fenomeno inedito. Il meccanismo di percezione delle distanze dell'internauta di oggi è lo stesso del londinese o del parigino che nell'Ottocento scendeva nella metropolitana e in pochi minuti percorreva una distanza che altrimenti avrebbe richiesto ore di cammino. La differenza è che mentre il viaggio dell'utente della metropolitana interconnette due dimensioni spaziali di cui una pienamente esperibile (quella dei luoghi fisici in superficie, mentre l'altra, quella sotterranea, gli rimane più difficile da cogliere), l'internauta si muove unicamente in una dimensione fuori dal controllo dei suoi sensi e dunque fuori dalla sua esperienza fisica. In pratica, l'internauta non può avvalersi di quei punti di riferimento reali di cui beneficia invece l'utente della metropolitana e questa circostanza amplifica la sua sensazione di muoversi in uno spazio astratto e sconfinato.

Fonte figura 1: C. LUESCHER, O. REICHENSTEIN, T. TANKA, M. GERBER, *Web Trend Map*, iA-Information Architects, Berlino-Zurigo-Tokyo 2007.

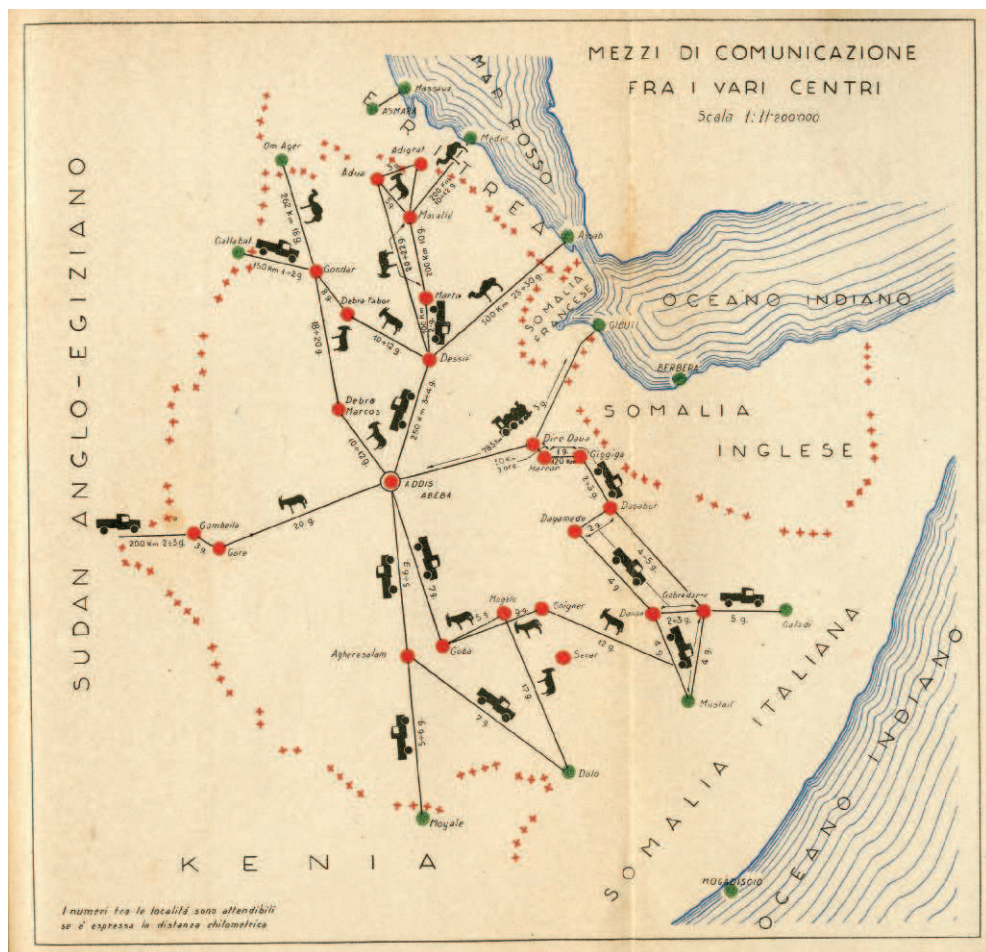
Fonte figura 2: L. MACDONALD GILL, *Cable e Wireless Great Circle Map. Britain the World Centre*, London 1945, Edward Stanford.

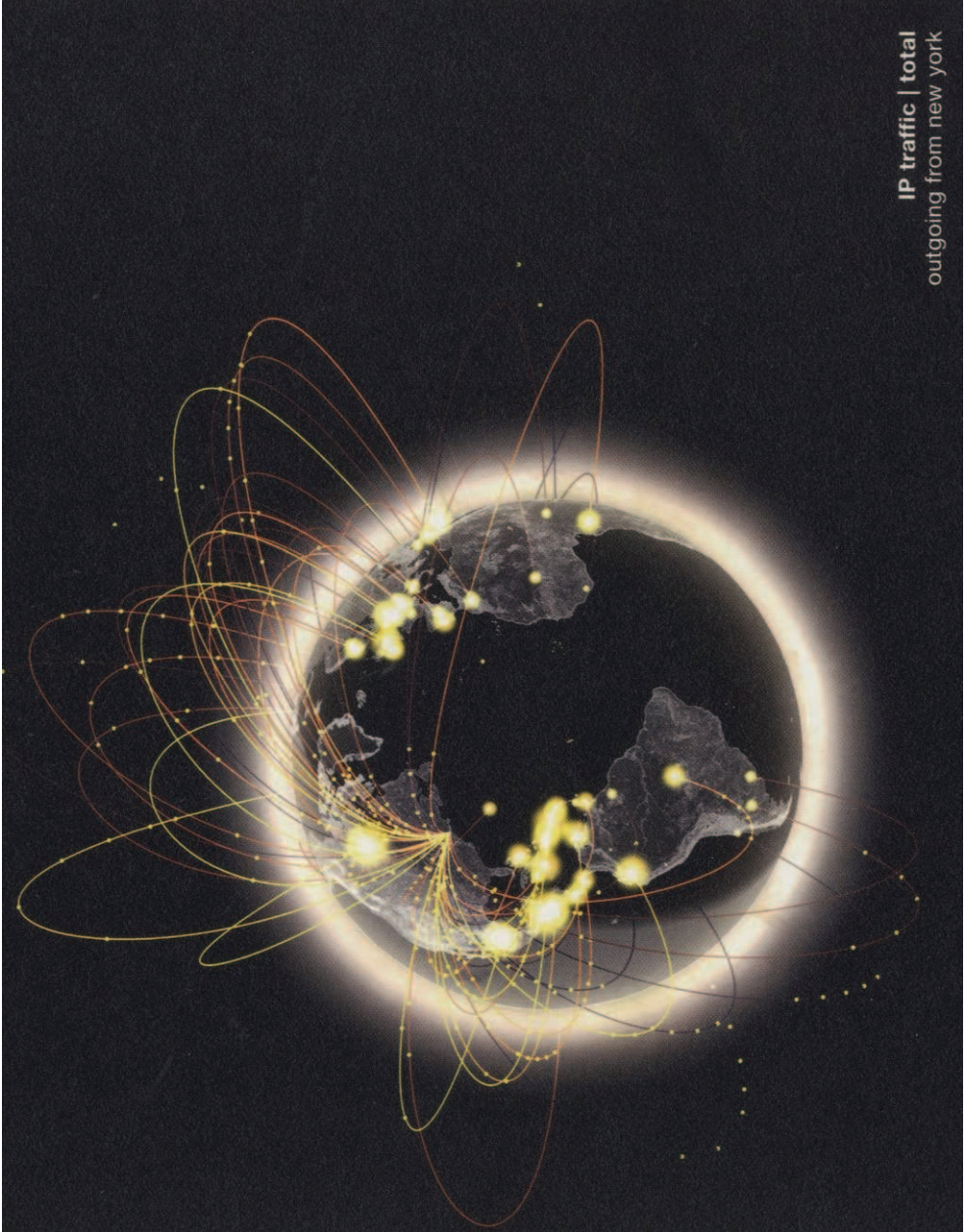
Fonte figura 3: «Mezzi di comunicazione fra i vari centri», da *Etiopia. Notizie schematiche sull'ordinamento politico-militare*, ministero della Guerra. Servizio Informazioni Militari, aprile 1935.

Fonte figura 4: *IP traffic | total outgoing from New York*, installazione interattiva MIT SENSEable City Lab, per la mostra «Design and the Elastic Mind» al MoMA di New York, 2008.









IP traffic | total
outgoing from new york

Ci sono sfide dove la velocità da sola non basta.



Filippo Tortu
Primatista italiano dei 100 m

146 | FASTWEB.IT | PUNTI VENDITA

FASTWEB
un passo avanti

Together
to 2020

IL FUTURO È
5G

L'ENERGIA DELLA TUA CASA È INTELLIGENTE?

Arriva OPEN METER, il contatore elettronico di seconda generazione. Un'innovazione tecnologica che E-Distribuzione sta portando nelle case degli italiani per consentire una gestione più consapevole dei consumi, impegnandosi ogni giorno affinché l'innovazione sia alla portata di tutti. **Perché qualunque essa sia, tu possa credere nella tua energia.**

E-Distribuzione ha già installato più di 6 milioni di contatori elettronici di nuova generazione nei Comuni Italiani e progressivamente saranno coinvolti tutti i 32 milioni di clienti connessi alla rete elettrica.

Scopri tutte le funzionalità, i vantaggi e quando Open Meter arriverà nel tuo Comune e a casa tua sul sito e-distribuzione.it o chiama l'800 085 577.



e-distribuzione.it

e-distribuzione